CONFERENCE MANUAL

DAY ONE

SPONSORED BY:

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON LAW & NATIONAL SECURITY

CENTER FOR NATIONAL SECURITY LAW
UNIVERSITY OF VIRGINIA SCHOOL OF LAW

CENTER ON LAW, ETHICS AND NATIONAL SECURITY
DUKE UNIVERSITY SCHOOL OF LAW

CENTER ON NATIONAL SECURITY AND THE LAW
GEORGETOWN LAW

NOVEMBER 14 — NOVEMBER 15, 2016

THE CAPITAL HILTON
1001 16TH STREET, NW
WASHINGTON, D.C.
# Conference Material: Day One

## Panel I
**The DOD Law of War Manual: Debate, Discussion and Developments in International Humanitarian Law 2015-2016**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DoD <em>Law of War Manual</em> and its Critics: Some Observations — Charles Dunlap, Jr.</td>
<td>1</td>
</tr>
<tr>
<td>Off Target: Selection, Precaution, and Proportionality in the DoD <em>Manual</em> — Adil Ahmad Haque</td>
<td>37</td>
</tr>
<tr>
<td>Common Article 1 to the Geneva Conventions and the obligation to prevent international humanitarian law violations — Knut Dörmann and Jose Serralvo</td>
<td>93</td>
</tr>
</tbody>
</table>

## Panel II
**The National Security Process and Structure**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Framework for the U.S. use of Military Force since 9/11 — Stephen Preston</td>
<td>223</td>
</tr>
<tr>
<td>Charlie Savage and the NSC Lawyers Group — John Bellinger</td>
<td>319</td>
</tr>
<tr>
<td>The Obama Administration and International Law — Harold Hongju Koh</td>
<td>321</td>
</tr>
<tr>
<td>International Law, Legal Diplomacy, and the Counter-ISIL Campaign — Brian Egan</td>
<td>331</td>
</tr>
<tr>
<td>Goldwater-Nichols at 30: Defense Reform and Issues for Congress — Kathleen McInnis</td>
<td>343</td>
</tr>
<tr>
<td>Don’t Rush to “Fix” Goldwater-Nichols — Justin Johnson</td>
<td>405</td>
</tr>
<tr>
<td>Joint Staff Director Describes Military Advice Process — Jim Garamone</td>
<td>409</td>
</tr>
<tr>
<td>10 U.S. Code §151</td>
<td>411</td>
</tr>
</tbody>
</table>

## Panel III
**Cyber Challenges for the New Administration**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why is the President downplaying alleged Russian attempts to influence U.S. elections? Maybe he doesn’t oppose all efforts to impact foreign voters — Charlie Dunlap</td>
<td>417</td>
</tr>
<tr>
<td>Can litigation against social media platforms help disarm terrorist organizations? — Charlie Dunlap</td>
<td>421</td>
</tr>
<tr>
<td>Have government lawyers “winced” at “cyber bomb” statements? If so, it may be about norm development — Charlie Dunlap</td>
<td>423</td>
</tr>
<tr>
<td>Cyber Sovereignty: The Way Ahead — Eric Talbot Jensen</td>
<td>427</td>
</tr>
</tbody>
</table>
### Panel III
(Cont’d)

**Cyber Challenges for the New Administration**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Attacks: Proportionality and Precautions in Attack — Eric Talbot Jensen</td>
<td>455</td>
</tr>
<tr>
<td>Executive Order 12333 United States Intelligence Agencies</td>
<td>469</td>
</tr>
<tr>
<td>National Insider Threat Policy</td>
<td>485</td>
</tr>
<tr>
<td>Executive Order 13636 Improving Critical Infrastructure Cybersecurity</td>
<td>495</td>
</tr>
<tr>
<td>Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing</td>
<td>505</td>
</tr>
<tr>
<td>Executive Order 13694 Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities</td>
<td>511</td>
</tr>
<tr>
<td>Draft Chapter Eighteen: Legal — Harvey Rishikof and Conor Sullivan</td>
<td>515</td>
</tr>
<tr>
<td>Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics — Harvey Rishikof and Kelly Russo</td>
<td>525</td>
</tr>
<tr>
<td>Cybersecurity, Elections, and Critical Infrastructure at Home and Abroad — Kristen Eichensehr</td>
<td>549</td>
</tr>
<tr>
<td>Risky Business: When Governments Do Not Attribute State-Sponsored Cyberattacks — Kristen Eichensehr</td>
<td>551</td>
</tr>
<tr>
<td>Resolution — American Bar Association Cybersecurity Legal Task Force</td>
<td>555</td>
</tr>
<tr>
<td>Cybersecurity Whistleblowing is Murkier Than You May Think — Renee Phillips and Shea Leitch</td>
<td>571</td>
</tr>
</tbody>
</table>

### Panel IV

**Refugees, Humanitarian Challenges and the Law**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Sponsorship of Refugee Resettlement in the United States: Guiding Principles and Recommendations — Human Rights First</td>
<td>577</td>
</tr>
<tr>
<td>The Syrian Refugee Crisis and the Need for U.S. Leadership — Human Rights First and Ryan Crocker</td>
<td>597</td>
</tr>
<tr>
<td>Respecting Rights and Securing Solutions — Human Rights First</td>
<td>641</td>
</tr>
<tr>
<td>Global Crises Are Overshadowing Hate Crimes — Jonathan Greenblatt and Elisa Massimino</td>
<td>667</td>
</tr>
<tr>
<td>The Syrian Refugee Crisis Won’t Be Solved with Small Gestures — Jonathan Greenblatt and Elisa Massimino</td>
<td>671</td>
</tr>
</tbody>
</table>
Panel I:

The DoD Law of War Manual: Debate, Discussion and Developments in International Humanitarian Law
2015-2016

Moderator:
James E. Baker
The DoD Law of War Manual and its Critics: Some Observations

Charles J. Dunlap, Jr

92 Int'l L. Stud. 85 (2016)

Volume 92 2016
The DoD *Law of War Manual* and its Critics: Some Observations

*Charles J. Dunlap, Jr*²

**CONTENTS**

I. Introduction ................................................................. 85  
II. Human Shields ............................................................... 87  
III. Precautions in Attack .................................................... 101  
IV. Morality, Honor, and the Collapse of Reciprocity .................. 103  
V. Journalists ................................................................. 107  
VI. Cyber ................................................................. 113  
VII. Conclusion ............................................................... 115

I. INTRODUCTION

When the Department of Defense (DoD) issued its *Law of War Manual* in June of 2015¹—an effort decades in the making—it is clear that it anticipated criticism. For an organization not especially disposed to be humble about its accomplishments, it made a surprising invitation in the text for “comments and suggestions.”² Several experts (and other pundits) have taken up

---

¹ Major General, USAF (Ret.), Professor of the Practice of Law and Executive Director of the Center on Law, Ethics and National Security at Duke University School of Law, https://law.duke.edu/fac/dunlap/.

² The thoughts and opinions expressed are those of the author and not necessarily of the U.S. government, the U.S. Department of the Navy or the U.S. Naval War College.


2. Id. at vi.
that offer, and have done so publically. Indeed, two major national/international security law-focused blogs, *Just Security* and *Lawfare*, created sections within their websites devoted to the *Manual*.

Many observers had been concerned about what the final product might look like. Hays Parks, the now-retired Marine and long-time DoD lawyer whom most experts consider to be his generation’s dean of law of war specialists, shepherded the project for almost three quarters of its two-decade development, and had expected it to be fielded sometime in 2010. However, progress on the *Manual* was abruptly halted that year when the Department of Defense decided to re-engage the inter-agency process, reportedly in deference to some political appointees in the Obama Administration who “aggressively sought changes in the DoD Manual to conform to their political philosophies or legal arguments in detainee litigation.” This led to fears by Parks and others that the final document would be mired in politics and reflect incorrect interpretations of the law that could “endanger the lives of [U.S.] fighting men and women.”

Those fears appear to have been largely avoided in the *Manual*, notwithstanding other criticisms that have arisen. The purpose of this article is to examine some of those critiques, and to offer, where appropriate, counters to those assessments, as well as suggestions as to how the *Manual* might be improved. Although this article does not purport to be a comprehensive examination of every aspect of the *Manual* or, for that matter, a response to every criticism that has been lodged against it, I nevertheless conclude that on balance the *Manual* provides an excellent, comprehensive and much-needed statement of the U.S. Department of Defense’s view of

---

7. Id.
the *lex lata* of the law of war. Consequently, with a few exceptions, what follows is generally a defense of the *Manual* pertaining to several issues that have proven to be contentious.

II. Human Shields

One of the most energetic and derisive of the *Manual*’s early critics is Professor Adil Ahmad Haque of Rutgers Law School. Just weeks after its release, he alleged on the *Just Security* blog that based on his reading of the text, the DoD “apparently thinks that it may lawfully kill an unlimited number of civilians forced to serve as involuntary human shields in order to achieve even a trivial military advantage.”

I responded by arguing a number of points, beginning by dismissing Haque’s interpretation of what he thinks the *Manual* asserts. What the *Manual* actually says about human shields is to repeatedly make the point that using them is prohibited by international law. It reflects the indisputable axiom that “civilians must not be used as shields or as hostages.” It further makes it clear that civilians, including human shields, must not be made the object of an attack.

Importantly, contrary to what Haque’s post suggests, the *Manual* does not exempt the U.S. military from the affirmative duty “to take feasible precautions to reduce the risk of harm to the civilian population and other protected persons and objects” and to incorporate such precautions “when planning and conducting” attacks. More specifically, the *Manual* insists that “wanton disregard for civilian casualties or harm to other protected persons and objects is clearly prohibited.”

---

8. See, however, notes 151 and 152, infra, and accompanying text (arguing that the *Manual*, by its own terms, does not necessarily speak for the entire U.S. government).
12. Id. ¶¶ 2.5.3.3, 5.16.3, 10.5.1.4, 11.6.1.
13. Id. ¶ 5.3.2.
14. Id. ¶ 5.3.3.
15. Id. ¶ 5.3.3.2.
The *Manual* does recognize that “in some cases, a party to a conflict may attempt to use the presence or movement of the civilian population or individual civilians in order to shield military objectives from seizure or attack.”\(^{16}\) It counsels however—*and this is critical*—that when “enemy persons engage in such behavior, commanders should continue to seek to discriminate in conducting attacks and to take feasible precautions to reduce the risk of harm to the civilian population and civilian objects.”\(^{17}\)

Regarding, human shields in particular, the *Manual* states:

> Harm to Human Shields. Use of human shields violates the rule that civilians may not be used to shield, favor, or impede military operations. The party that employs human shields in an attempt to shield military objectives from attack assumes responsibility for their injury, provided that the attacker takes feasible precautions in conducting its attack.

> If the proportionality rule were interpreted to permit the use of human shields to prohibit attacks, *such an interpretation would perversely encourage the use of human shields* and allow violations by the defending force to increase the legal obligations on the attacking force.\(^{18}\)

So Haque’s overstated accusation is *legally* deficient as there are plenty of precautions aimed at protecting civilians memorialized in the *Manual*’s text. I also suggested that regardless of where one might stand on the *Manual*, should we not all be concerned that nowhere in his legal analysis does Haque even mention “feasible precautions” despite it being embedded (repeatedly) in the *Manual* as a legal requirement? I asked, rhetorically, is that not a pretty significant omission? And, of course, it is.

Haque dismisses DoD’s common-sense view that allowing unscrupulous defenders to succeed in deterring attacks through the use of human shields would “perversely encourage the use of human shields.” He contends that:

> [A]ttacking combatants despite the presence of involuntary shields will not make those combatants any worse off than they would have been without those shields. On the contrary, if defending forces expect addi-

\(^{16}\) *Id.* ¶ 5.5.4.

\(^{17}\) *Id.* (emphasis added).

\(^{18}\) *Id.* ¶ 5.12.3.3 (emphasis added).
tional (say, political) benefits and no additional costs from using involuntary shields then killing these involuntary shields will not deter their use.\(^{19}\)

If you accept this logic, then you are buying into the idea that even if targets come to accept that they will not be protected from attack by surrounding themselves with human shields, they will nevertheless continue to burden themselves by acquiring, guarding, feeding, housing and otherwise supporting human shields. Moreover, they will do so even though the very presence of human shields increases their “footprint” (and therefore their chances of being detected by a variety of surveillance capabilities), diminishes their own reputation for fearlessness, risks strategic “backfire,”\(^ {20}\) hardens public opinion against them\(^ {21}\) and can put them in conflict with religious beliefs.\(^ {22}\) In truth, there are considerable costs to keeping human shields, especially under circumstances where they would not, in fact, actually constitute a shield.

Nevertheless, Haque speculates that targets still would perceive that they could “expect” additional “political” benefits from keeping human shields, presumably from propagandizing those who might be killed in strikes. This is wrong for two reasons: one, thanks to advances in technology, targets can no longer assume that simply being close to civilians will mean that civilians will die in an attack (consider that even though terrorists targeted in drone operations have tried to do just that, civilian fatalities from drone strikes are actually rare these days\(^ {23}\)); and, secondly, even when hostages are killed in attacks (as was the case in 2015), public support for such strikes remains strong despite concerns among the populace that the attacks could endanger the lives of innocent Americans.\(^ {24}\)

\(^{19}\) Haque, *The Defense Department’s Indefensible Position*, supra note 10.


In his responses to my critique, Haque argues that I have a "utilitarian argument" as to the importance of avoiding incentivizing an enemy to use human shields.25 Not so, except perhaps to say I see great utility in not allowing the law of war (LoW) to incentivize activities that put civilians at risk. In my view one of the underlying purposes of the LoW is, as the Manual puts it, "protecting combatants, noncombatants, and civilians from unnecessary suffering,"26 and it should be interpreted towards that end. I disagree with Haque's conclusion that the LoW mandates allowing a belligerent unimpeded use of human shields, subject only to some theoretical after-the-fact accountability for war crimes.

In fact, I believe it is not improper for an attacker to consider the protection of civilians as well as the importance of maintaining adherence to the LoW as part of the "definite military advantage sought" in conducting a proportionality analysis.27 Along this line, the Manual notes that the Final Report of the Persian Gulf War concluded that military advantage "is not restricted to tactical gains, but is linked to the full context of a war strategy, in this instance, the execution of the Coalition war plan for liberation of Kuwait."28

Acting to preserve the LoW operates broadly as a strategy not just as a philosophical good, but also a very practical way to deny the enemy the ability to effectively use human shields as a method of warfare in its military operations. Doing so offers a definite military advantage to the attacker—not to mention civilians—over the longer term. Importantly, as the Manual makes clear, international law does not require that the "advantage" be "immedi-
ate,"
and that advantage is "not restricted to immediate tactical gains, but
may be assessed in the full context of the war strategy."

We can never forget that voluntary and involuntary human shields un-
dermine the fundamental law of war principle of distinction and the pro-
tection of innocent civilians. The real issue is what works best to protect
civilians? Here is where the Manual could be clearer. It would be better to
explicitly point out that, as described above, when an attack is designed at
least in part to deny an adversary the military advantage of using human
shields as a method of warfare, that end constitutes a powerful strategic mili-
tary advantage for the attacker to seek and is, therefore, quite significant in
determine what might be feasible in the protection of civilians.

Subsequent to this colloquy, two more notable posts appeared on the
Just Security blog about human shields. The first, with the very intriguing
title Human Shields: Weapon of the Strong, is co-authored by Professor Neve
Gordon, a political scientist at Ben-Gurion University, and Brown University
anthropologist, Professor Nicola Perugini. In their essay they bring an
extraordinarily useful interdisciplinary voice to the dialogue by critiquing
both Haque and me by contending that we “both treat human shielding as
an ahistorical phenomenon and therefore fail to address a much more fun-
damental question: Why does the Law of War Manual suddenly include
clauses dealing with human shields?”

They argue that “human shielding is not a new phenomenon” and go
on to propose an answer to their own question by saying:

29. Id., ¶ 5.7.7.3 (citing J. Fred Buzhardt, DoD General Counsel, Letter to Senator
Edward Kennedy, Sept. 22, 1972, reprinted in 67 AMERICAN JOURNAL OF INTERNATIONAL
LAW 122, 124 (1973)) (“Turning to the deficiencies in the Resolutions of the Institut de
Droit International, and with the foregoing in view, it cannot be said that Paragraph 2,
which refers to legal restraints that there must be an ‘immediate’ military advantage, re-
flects the law of armed conflict that has been adopted in the practices of States.”).

30. Id., ¶ 5.7.7.3. (footnote omitted) (citing conduct of the persian gulf war:
final report on to congress 613 (1982) (“Military advantage is not restricted to
tactical gains, but is linked to the full context of a war strategy, in this instance, the execu-
tion of the Coalition war plan for liberation of Kuwait.”)). See also William H. Boothby,
the law of targeting 189 n.70 (discussing the statement made by the UK in ratifying
additional protocol I to the geneva conventions); Ian Henderson, the contempo-
rary law of targeting 64 (2009).

31. Neve Gordon & Nicola Perugini, human shields: weapon of the strong, just secu-
ritv (Oct. 22, 2015), https://www.justsecurity.org/27005/human-shields-weapon-stro-
ng/.
Our counterintuitive hypothesis is that human shields are not only being deployed as a weapon of the weak against high tech states (the underlying assumption of both Haque and Dunlap), but that the legal phrase “human shield” has also been mobilized by strong states to legitimize the increasing deaths of civilians on the battlefield.\textsuperscript{32}

Gordon and Perugini, who sponsored a workshop on this subject,\textsuperscript{33} are certainly correct in that human shields have been used in the past. Yet frequency of a particular issue does matter when military manuals are being written. With respect to human shields, Professor Michael Schmitt in his work on the subject says the phenomenon is “endemic in contemporary conflict,”\textsuperscript{34} but also cites a quote from Jean Pictet’s 1958 commentaries on the Geneva Conventions, which said at that time that such instances were “fortunately rare.”\textsuperscript{35} Something rare in the past would logically and understandably be treated more extensively when it becomes “endemic” simply as a matter of military practicality as opposed to any nefarious reasons.

Regardless, military professionals and others who would use the \textit{Manual} would likely not be surprised as to why it addresses the phenomenon in more detail than did previous documents. Previous use of human shields just did not prove to be the deterrent to attack that they have become today (this is likely why the instances were, in Pictet’s assessment, “rare”). Why the change? The truly unprecedented sensitivity to \textit{any} civilian casualties that we see in current operations simply did not exist in earlier eras. And that sensitivity is not, particularly, because of new legal impediments, \textit{per se}, but because of \textit{policy} restraints much beyond what the LoW requires.

As I have discussed in \textit{War on the Rocks}, the Obama Administration created—and publicized—policy standards for the use of force in counterterrorism operation outside of what it calls “areas of active hostilities” that demand not just a determination (as international law would have it) that the expected casualties not be “excessive” in relation to the anticipated military advantage, but rather a “near certainty” that \textit{no} civilian casualties will

\textsuperscript{32} Id.
\textsuperscript{33} The workshop, entitled “The Politics of Human Shielding” took place at Brown University (RI) on November 17, 2015.
\textsuperscript{34} Michael N. Schmitt, \textit{Human Shields in International Humanitarian Law}, 38 \textbf{ISRAEL YEARBOOK ON HUMAN RIGHTS} 17, 18 (2008).
\textsuperscript{35} \textit{COMMENTARY TO GENEVA CONVENTION IV RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR} 208 (Jean Pictet ed., 1958).
occur.\textsuperscript{36} I observed in that essay that while human shields were "a serious violation of international law," this was "hardly an impediment to al-Qaeda, especially if violating it might ensure policy-induced protection against airstrikes or other uses of force."\textsuperscript{37} Though the Administration said in the fall of 2014 that the restrictive policies would not apply to operations against the Islamic State in Iraq and Syria (ISIS), it appears that equally limiting standards have nevertheless been in place.\textsuperscript{38}

Predictably, given the openly announced standards, today's adversaries have concluded that using human shields will "work" because they assume—for understandable reasons—that the human shields will protect them from attack, or if they are attacked, to give them a propaganda windfall. As a Syrian activist recently put it, ISIS "uses civilians as human shields to claim that the U.S.-led coalition is targeting innocent people during the strikes."\textsuperscript{39}

ISIS's use of human shields is an expression of a version of what I call "lawfare," whereby a party to a conflict creates the perception of illegality in order to serve a belligerent purpose.\textsuperscript{40} In other words, as opposed to Gor-


\textsuperscript{37} Id.

\textsuperscript{38} See Michael Isikoff, \textit{White House Exempts Syria Airstrikes from Tight Standards on Civilian Deaths}, \textit{Yahoo News} (Sept. 30, 2014), http://news.yahoo.com/white-house-exempts-syria-airstrikes-from-tight-standards-on-civilian-deaths-183724795.html. However, recent news reports indicate that very tight standards are, in fact, being applied:

A senior American official said every air strike, whether conducted by a fighter jet or unmanned aerial vehicle, night or day, must be cleared by an American general officer. In order to strike a building it has to be determined that it is "sole use ISIS," meaning there must be certainty that the enemy is not co-mingling there with civilians. "We aim for zero collateral damage," said one young officer in the CJCOC.


andon and Perugini's interpretation of the discussion in the Manual, the use of human shields at various times in the past simply never developed into the reliably effective military tactic that needed to be addressed as it does today. The fact is that such abuse of civilians did not necessarily deter attackers in earlier eras, and the employers of human shields were vulnerable to having their own people treated similarly. It rarely worked then; it often works now.

Furthermore, the pervasiveness of twenty-first century information technologies simply did not exist in previous wars. Belligerents lacked the technical means to rapidly and effectively exploit the deaths of the human shields as easily as they can today. That reality, combined with the fact that in earlier eras human shields did not deter most attacks, can readily explain why human shields were not discussed as they are in the new Manual. Personally, I have never heard anyone—let alone a military professional—suggest anything remotely along the “legitimize civilian deaths” lines as Gordon and Perugini hypothesize.

This raises a further issue with Gordon’s and Perugini’s hypothesis: the complete absence of any evidence that indicates any sort of norm is arising demonstrating that the so called “strong States” have “mobilized” the human shields phenomenon to “legitimize the increasing deaths of civilians on the battlefield.” That said, Gordon and Perugini may be extrapolating from their view of Israel’s operations in Gaza to a supposition about “strong States” more generally.41

At the risk of oversimplification, my sense is that Gordon and Perugini have concluded that Israel has essentially declared the entire area of Gaza as one where all civilians are being actively used as human shields. This characterization, they seem to contend, has allowed Israel not only to declare all civilian deaths as result of Israeli attacks the responsibility of the Hamas defenders for illegally using human shields, but also to permit Israel to relieve itself of the targeting precautions—to include any proportionality analysis—that the LoW would otherwise require in most circumstances. I do not read the DoD Manual as endorsing such a broad interpretation of human shielding, but I gather Gordon and Perugini do.

To be clear, I am not necessarily agreeing with what seems to be their interpretation of Israel's use of force in Gaza, but if accurate, Israeli actions would be hard to square with the law. Rather, I believe that even if true, Israel's actions are not themselves enough to establish an international norm vis-à-vis human shields. Personally, I view much of the legal aspects of the Israeli-Palestinian situation as sui generis, and of limited LoW application beyond its rather specific and unique circumstances.

In any event, the United States has instituted policies—as wrong-headed (albeit well-intended) as they may be—that are plainly just the opposite—that is, aimed at the quixotic goal of a “near certainty” of zero civilian deaths, not any “legitimization” of them. These overly restrictive policies—expressed in rules of engagement—have actually inhibited the application of force against, for example ISIS, that would otherwise be permitted by international law.

Moreover, it has always been the case since 9/11 that the vast majority of civilian casualties have not been caused by “strong States.” To the contrary, it is adversaries whose disregard for international law typically goes beyond merely the unlawful use of human shields that are overwhelmingly responsible. For example, in its August 2015 report about civilian deaths in Afghanistan, the UN “documented a 78 per cent increase in civilian casualties attributed to Anti-Government Elements from complex and suicide attacks and a 57 per cent increase in civilian casualties from targeted kill-


43. See, e.g., John Hayward, Impossible Rules of Engagement: “Zero Civilian Casualties” in ISIS Battle, BRETTBART (June 24, 2015). In addition, consider:

In Iraq and Syria today, the US operates under a zero civilian casualty standard that far exceed the standards of international law. That policy is backfiring—it is extending the time to secure military objectives; allows more time for the Islamic State to commit atrocities; more radical Islamists to emerge out of Syria; and it yields the Islamic State the equivalent of an air defense capability they do not have to pay for, equip, or man to employ. Moreover, this excessive caution is sparking a crisis in confidence that has invited further violence emboldening others to take action not aligned with US interests. Russian intervention in Syria is an obvious example, and the attacks in Paris are the most recent manifestation of a timid and feckless coalition strategy.

ings." The UN also "attributed 94 per cent of all civilian casualties from targeted killings to Anti-Government Elements."5

The facts are glaringly inappposite of Gordon's and Perugini's contentions, and just do not support the idea that the United States as a "strong State" is responsible for "increasing deaths of civilians on the battlefield."46 Indeed, as grim as the statistics are, they serve as an empirical counterpoint to any supposed American effort at "legitimization" of civilian causalities. Indeed, it is evidence that the view of human shields as reflected in the Manual is not interpreted or used by U.S. forces to accomplish the nefarious end Gordon and Perugini allege, notwithstanding whatever may be the case with the Israelis.

The second of the new postings on this topic was by Haque himself.47 While he applauded Gordon and Perugini's essay, he went on to speculate that the current Manual approach to human shields is somehow sourced in a 1990 law review article authored by Hays Parks, the renowned Low expert I mentioned above.48 Suffice to say, absent explicit evidence linking him to the Manual's construct, I would not conclude that Parks—who retired from the government in 2010 and who has declined to read the Manual—had anything to do with drafting this section of it (even assuming Haque is correct in his analysis of the Parks article).49 As I have pointed out elsewhere, the language to which he objects comes from a 1991 State Department response to the International Committee of the Red Cross.

44. To be clear, of the total civilian deaths, 70 percent were caused by anti-government elements, 16 percent by pro-government forces, 10 percent unattributed and 4 percent other. See UN Assistance Mission to Afghanistan & UN Office of the High Commissioner for Human Rights, Afghanistan Mid-Year Report 2015: Protection of Civilians in Armed Conflict, 3 (Aug. 2015), http://www.ohchr.org/Documents/Countries/AF/UNAMA_Protection_of_Civilians_in_Armed_Conflict_Midyear_Report_2015.docx.

45. Id. at 8.


48. Id. The article to which Haque refers is W. Hays Parks, Air War and the Law of War, 32 AIR FORCE LAW REVIEW 1 (1990).

49. Parks' article is cited elsewhere in the Manual. I would not conclude that the current construct is his invention. See DOD MANUAL, supra note 1, ¶ 15.5.4 n.85.

(ICRC). Unless Parks or the Manual drafters state otherwise, Haque’s contention remains in the realm of imagination.

Haque also claims that the Manual’s “position” is that “civilians forced to serve as human shields can never render an attack unlawfully disproportionate, no matter how great the expected harm to those civilians or how small the anticipated military advantage.” Yet nowhere does he cite any text that actually states this alleged “position.” More importantly, it diametrically conflicts with the Manual’s many statements requiring attackers—including where human shields are involved—to use all feasible precautions to prevent harm to civilians.

Allow me to clarify my construct for the Manual’s view of human shields that considers the proportionality analysis certainly differently than Haque, but perhaps even differently that the Manual drafters. Briefly, I suggest that where the object of an attack is the military force employing human shields, and the military necessity for doing so rests not so much on the desire to halt the use of human shields because it is an inhuman and illegal action, per se, but rather because the use of human shields has become in a given conflict a regularized, explicit and effective method of warfare for a particular enemy, the calculus necessarily changes, and perhaps even dramatically so.

Consequently, the proportionality analysis as to what might be excessive in order to achieve that specific anticipated military advantage (that is, halting the enemy’s use of a tactic that may have shown real success in discouraging the use of force against them), would fit within that extant mandate of the Manual to do everything “feasible” to avoid harm to human shields. Put another way, given the military purpose involved, the proportionality calculation could be quite different as to what it may take to end the military utility of using human shields—as well as what would be “feasible” under those circumstances to protect them. In short, the assessment

51. Haque, Human Shields in the DOD Manual, supra note 47.
52. See, e.g., DOD MANUAL, supra note 1, ¶ 5.12.3.3.
54. Cf. Boothby, supra note 30, at 137 (“[T]he proportionality assessment must still be undertaken in cases where there are involuntary human shields in the vicinity of intended target of the attack, the better view is that the increased numbers of expected civilian casualties will not necessarily be excessive given the deliberate placing of civilians there.”) (citations omitted).
55. Id.
must necessarily take into account the atypical circumstance where the use of civilians as human shields intensifies into a significant military advantage for an unscrupulous defender. If the utility of human shields—and the consequent risk to civilians—is to be blunted, it needs to be unambiguously established militarily that the use of human shields will not, in fact, prevent an attack on any forces employing them.

This approach is related to the concept of reprisal, but not conterminous with it. Obviously, it does not involve—or permit—targeting human shields directly, but it also does not depend upon determining whether the human shields are truly voluntary or not—something that may be a practical impossibility, especially with respect to aerial attacks. Causing an adversary to abandon this method of warfare can produce a concrete and direct military advantage that also serves to protect civilians who might otherwise be employed as human shields were the tactic allowed to be effective.

There are, however, much more orthodox explanations for the Manual’s approach, and that is the time-honored norm of international law that there are certain categories of persons—munitions workers for example—whose proximity to an otherwise legitimate target is “understood not to prohibit attacks under the proportionality rule.” Specifically, the Manual restates the long-standing U.S. view that a “party that employs human shields in an attempt to shield military objectives from attack assumes responsibility for their injury, provided that the attacker takes feasible precautions in conducting its attack.”

Understandably, one might want to distinguish (as this writer would like to do) between voluntary and involuntary human shields, but the chaos of battlefield reality is such that delineations among civilians are not any more feasible to make than would be the case with voluntary/involuntary munitions workers. It is also important to recall with respect to voluntariness, the LoW—as Butch Bracknell recently noted—makes no exception for non-volunteers conscripted into a belligerent’s armed forces. They are subject to targeting under the LoW simply because of their status, even if it could be conclusively shown that their military service is involuntary.

56. DOD MANUAL, supra note 1, ¶ 5.12.3.2.
57. Id., ¶ 5.12.3.3.
Still, under the LoW does an involuntary civilian human shield have distinct individual rights independent of the behavior of belligerents? No, that is simply not how the *lex specialis* of the LoW works as it mainly concerns *parties* to a conflict, not the private rights of individuals. Even if the LoW was somehow rejiggered to be individual human rights-centric, it is not clear that the apparently preferred outcome of Haque, Gordon and Perugini for human shields would result. One would also have to consider the individual human rights of combatants to live, not to mention the rights of civilians who would be imperiled by the continued unrestrained use of human shields.

Moreover, critics seem to want a LoW rule that would, in effect, permit a clever and unprincipled adversary with access to enough human shields to create a legal “fortress” around all or a significant part of his critical military capability where virtually any attack would be legally prohibited. To reward a belligerent for flaunting the LoW in that way is flatly contrary to the principle of international law expressed in the axiom *ex injuria non jus oritur* or “legal rights should not be understood to result from the commission of wrongful acts.”

This does not mean, as Gordon and Perugini seem to fear, that the entire battlespace can be transformed into an area where the normal proportionality rules and other precautions do not apply irrespective of the actual location of specific military capabilities. Rather, it is to simply make the point that proliferate use of illegal human shields in a militarily significant way cannot be allowed to create a force of legally protected military objects that cannot be otherwise effectively struck. In this context, the “feasibility” determination would take into account how militarily important and effective the enemy’s use of human shields has become. If their use is sporadic, and the impact is only minimal in a particular situation, the “feasibility” requirement may markedly limit an attack or even bar it altogether.

This axiom is particularly relevant here because the critics do not offer any option for militaries confronted with the systematized use of human shields as a method of war except to expect them to accept whatever setbacks and even defeats that the illicit tactic can produce. This illegality is different from many other violations of the LoW such as, for example, the infliction of unnecessary suffering on combatants or even the targeting of civilians because it is aimed at achieving a definite and concrete military advantage, that is, the protection of military objects, via an illicit method.
International law recognizes that States will not accept tactical or, especially, strategic defeat because of some legal construct that allows a lawbreaker to use with impunity a criminal means to achieve victory over them.

More generally, the law understands that at the end of the day, even uniquely unpalatable and undesired actions may nevertheless be required. A form of this concept, I would argue, underlays the International Court of Justice’s opinion in the **Nuclear Weapons** case wherein the Court spent considerable time decrying the weapons but finally concluded that they could not say their use, as horrific as it might be, would be illegal under extreme circumstances.59

Of course, this is not to imply that the use of human shields would typically engage the exigencies of nuclear weapons use, but it does illustrate the importance of international law—and especially the LoW—remaining workable and sensible to law-abiding nations. A good example is how the 1936 London Charter60 regarding submarine warfare proved impractical in combat, and has been subsequently interpreted (not without some controversy) in a way that honorable nations are not disadvantaged.61 Given that the law has proven almost totally impotent in restraining today’s adversaries who routinely violate LoW in exquisitely barbaric ways, we should be very sensitive to—and resistant of—any reading of the LoW that seems to result in privileging such lawbreakers because of their lawbreaking. To do so would invite the unravelling of the LoW regime if States conclude it produces such anomalous—and dangerous—results.

There is no doubt that human shields represent a devilishly complicated issue with no perfect answers. In many, or most, cases a commander would not, for policy reasons, conduct an attack where human shields of any type exist. But the **Manual** principally aims not to make fact-dependent policy decisions, but rather to describe what existing law permits.

We already live in a world where the worst belligerents exhibit a stunning contempt for the LoW, and the **Manual**—very wisely in my judgment—avoids incentivizing their use of human shields, something that would be the inevitable result of the adoption of Haque’s view, as well as


that of Gordon and Perugini. It is imperative that the Low not be allowed to be manipulated by criminals so as to give de facto immunity to their military objectives. Such a situation would leave the fate of civilians to monsters whose very use of human shields clearly illustrates their gross indifference to human life.

III. PRECAUTIONS IN ATTACK

Professor Haque and I also clashed over his critique of the Manual's admittedly unartful reading of Article 57(3) of Additional Protocol 1 of the Geneva Conventions (AP I) (to which the United States is not a party). It deals with precautions commanders must take before attacking in order to avoid unnecessary harm to civilians. According to Haque, this Manual provision, which he seems to understand as a total rejection of the essence of Article 57(3), is “both legally and morally unsustainable.” His interpretation is one that the ICRC does not seem to share, but more about that in a minute.

In my response, entitled Let's Balance the Argument about the DOD Law of War Manual and Targeting, I began by inviting readers to look at the provision of the Additional Protocol so they may make their own judgment. The text of Article 57(3) provides:

When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.

Here is what the Manual says about that provision:

AP I provides that “[w]hen a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.” The United States has

62. Protocol I, supra note 27, art. 57(3).
64. Dunlap, Let's Balance the Argument, supra note 50. This section is largely taken from that post.
65. Protocol I, supra note 27, art. 57(3) (emphasis added).
expressed the view that this rule is not a requirement of customary international law.\textsuperscript{66}

With respect to the last sentence, the Manual provides a footnote that says in substance:

Paragraph 4B(4) contains the language of Article 57(3) of Protocol I, and is not a part of customary law. The provision applies “when a choice is possible . . . ,” it is not mandatory. An attacker may comply with it if it is possible to do so, subject to mission accomplishment and allowable risk, or be may determine that it is impossible to make such a determination.\textsuperscript{67}

Haque considers this citation to be a mere “Army statement” (perhaps because of a misleading footnote in the ICRC customary law study\textsuperscript{68}), but it is actually from the Digest of United States Practice in International Law 1991–1999.\textsuperscript{69} According to the State Department, the Digest is intended to “provide the public with a historical record of the views and practice of the Government of the United States in public and private international law.”\textsuperscript{70} This particular extract is from a January 11, 1991 telegram sent in response to a December 1990 memo that the ICRC distributed (to nations who might participate in the then pending Gulf war conflict) about the applicability of what the ICRC terms “International Humanitarian Law.”

In short, the position Haque criticizes is not a recent invention of DoD or the Army, but rather has been the view of the U.S. government for almost twenty-five years. Equally importantly, consider how the ICRC interprets the U.S. position in its study of customary international law:

Interpretation
The United States has emphasized that the obligation to select an objective the attack on which may be expected to cause the least danger to civilian

\textsuperscript{66} DOD MANUAL, supra note 1, ¶ 5.11.5 (emphasis added).
\textsuperscript{67} Id., ¶ 5.11.5 n.303 (emphasis added).
\textsuperscript{68} 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 67 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter CIHL Study].
lives and to civilian objects is not an absolute obligation, as it only applies "when a choice is possible" and thus "an attacker may comply with it if it is possible to do so, subject to mission accomplishment and allowable risk, or he may determine that it is impossible to make such a determination."\(^{71}\)

In other words, the ICRC does not relate the U.S. view as a wholesale rejection of the "obligation" but says that the view is merely an interpretation explicating the precise circumstances in which it applies, that is, "when a choice is possible." While the United States had—and continues to have—many objections to the ICRC study,\(^{72}\) this particular rendition of the U.S. view has not drawn complaints from the U.S. government.

You be the judge, but I do not think that the U.S. common-sense interpretation is "legally and morally unsustainable," and my bet is that others would agree. In fact, this may be why it has not generated much in the way of criticism over the years. The interpretation reflects, I would suggest, a keen understanding of the realities of war and hard experience in the importance of clarity about something that could easily be misunderstood (as it seems, Haque has done).

However, what may be a bona fide criticism of the Manual is that the ICRC interpretation may be a clearer and better explanation of the U.S. position, and ought to be considered for adoption in the next iteration of the Manual.

IV. MORALITY, HONOR, AND THE COLLAPSE OF RECIPROCITY\(^{73}\)

As can already be seen, part of my sparring with Professor Haque over human shields and targeting drifted into my objection to his characterization of various Manual provisions as "morally unintelligible," and to the charge that the assessments of the Manual's drafters had "no obvious basis" in "morality."\(^{74}\) I saw these remarks as ad hominem attacks on those who

\(^{71}\) CIHL Study, supra note 68, at 67 (emphasis added).


\(^{74}\) See Haque, The Defense Department's Indefensible Position, supra note 10.
take a different view as to how to accomplish what seems to be the same end sought by Haque: the protection of civilians.\footnote{Dunlap, Human Shields and the DOD Law of War Manual, supra note 11.}

Haque countered by insisting that “nowhere in [his] post [does he] question the character of the DoD Manual’s authors. [He says that he is] sure that they are fine people. Instead, [he] question[s] the soundness of the DoD Manual’s position.”\footnote{Haque, Human Shields and Proportionality, supra note 25.} When I answered by saying that you could not separate an attack on the morality of a position, from an attack on the author of it,\footnote{Dunlap, Let’s Balance the Argument, supra note 50.} he responded with a number of contentions, including the view that “[i]f morality were subjective—an expression of each individual’s emotions or preferences—then, indeed, all moral disagreement would be an exchange of personal attacks. However, morality is not subjective but objective, not an expression of how we feel but a reflection of how things are.”\footnote{Adil Ahmad Haque, DOD is Still Wrong about Target Selection and Civilians, JUST SECURITY (July 15, 2015), https://www.justsecurity.org/24671/dod-wrong-target-selection-civilians/.}

Still, Haque’s reference to morality is a worthy concern, and one in which I do find some of common ground with him when evaluated in a slightly different context. Regarding that context, consider the implications of what Creighton Professor Sean Watts calls a “significant recalibration” of law of war principles in the Manual, and one that “signals a return to very broad, generally applicable legal principles in a truer sense.”\footnote{Sean Watts, The DOD Law of War Manual’s Return to Principles, JUST SECURITY (June 30, 2015), https://www.justsecurity.org/24270/dod-law-war-manuals-return-principles.} Specifically, Watts is assessing the fact that while there have been several different listings of such principles over the years, the Manual settles upon “[t]hree interdependent principles—military necessity, humanity, and honor—as providing the foundation for other law of war principles, such as proportionality and distinction, and most of the treaty and customary rules of the law of war.”\footnote{DOD MANUAL, supra note 1, ¶ 2.1.}

To Watts, the inclusion of “humanity” is “perhaps its most drastic adjustment to existing doctrine.”\footnote{Watts, supra note 79.} He considers that the Manual’s “notion of humanity abandons recent refinements of that concept in favor of a more general approach.” But what he finds “most surprising” is the Manual’s “revival of the principle of honor” (which he uses, as the Manual does, in-
terchangeably with chivalry).\textsuperscript{82} Watts says the \textit{Manual} “sketches honor in exceedingly broad terms and applies it to an extensive range of battlefield conduct,” but questions the “practical utility of the principle.”\textsuperscript{83}

Professor Rachel VanLandingham has a harsher assessment saying she has a “visceral negative reaction” to the \textit{Manual’s} “emphasis on honor and chivalry.”\textsuperscript{84} In her mind they are “outdated, chauvinistic, and frankly distasteful concepts.”\textsuperscript{85} She also thinks that chivalry “connotes chauvinism, elitism, and the inhumanity of the Crusades,” adding that “codes of honor” signal “the assumed white, western, Christian superiority of the [era of the Crusades].”\textsuperscript{86}

While some elements of chivalry may have indeed had chauvinistic connotations, \textit{modern} concepts of battlefield honor can and do draw from a broader and deeper moral source that underpins the law of war. Professor Terry Gill of the University of Amsterdam and the Netherlands Defence Academy relates:

> Chivalry and martial honour have long been regarded as essential components of warrior ethics and military tradition. They are reflected in most cultures in one way or another, ranging from Western warrior tradition dating back to classic antiquity and medieval chivalry, to the various warrior codes of the ancient and medieval Near East, India, China and Japan. They also were practiced in various forms by many other cultures outside the arc of Eurasian/Mediterranean civilisation, including Native Americans and warrior peoples in Africa and the Pacific.\textsuperscript{87}

Michael Ignatieff makes a similar point in his classic book \textit{The Warrior’s Honor: Ethnic War and the Modern Conscience} where he notes that modern law of war conventions “drew upon a deeper moral source—the codes of a warrior’s honor.”\textsuperscript{88} Ignatieff explains that

\begin{itemize}
  \item \textsuperscript{82} Id.
  \item \textsuperscript{83} Id.
  \item \textsuperscript{84} Rachel VanLandingham, \textit{The Law of War is Not about Chivalry}, \textit{JUST SECURITY} (July 20, 2015), https://www.justsecurity.org/24773/laws-war-chivalry/.
  \item \textsuperscript{85} Id.
  \item \textsuperscript{86} Id.
  \item \textsuperscript{88} Michael Ignatieff, \textit{The Warrior’s Honor: Ethnic War and the Modern Conscience} 116–17 (1998).
\end{itemize}
Warrior’s honor was both a code of belonging and an ethic of responsibility. Wherever the art of war was practiced, warriors distinguished between combatants and noncombatants, legitimate and illegitimate targets, moral and immoral weaponry, civilized and barbarous usage in the treatment of prisoners and of the wounded. Such codes may have been honored as often in the breach as in the observance, but without them war is not war—it is no more than slaughter.99

Contrary to Watt’s bemusement about the inclusion of honor/chivalry in the Manual, and VanLandinghams’s apparent revulsion of it, I find real wisdom in what the Manual’s drafters have done. My reasoning is that doing so might help address the vacuum occasioned by the near disappearance of what was once a key supporting pillar of the law of war—reciprocity—from the kinds of conflicts in which military forces find themselves these days. Indeed, Watts and VanLandingham both allude to today’s phenomenon of belligerents who make it part of their way of fighting to flaunt non- adherence to the law of war. Witness ISIS’s horrific burning of a captive Jordanian pilot,90 and even more appalling, the crucifixion of children and their burial of them alive.91

The increasing irrelevance in practical terms of the concept of reciprocity should be of no small concern to advocates of the rule of law in war. Professor Ken Anderson of American University warned not long ago that “[o]bligation without reciprocity risks breakdown [of the rules of war] even faster where one side is pressed to protect the civilians of both sides put at risk because that’s how the other side deliberately wages war, not merely from indifference to them.”92 What is more, Anderson ominously predicts that in such circumstances:

A system of formal reciprocity in the rules of war (each side has the same formal obligations), but also independence of obligation to the rules of war (each side’s obligation is independent of what the other side does, in-

89. Id. at 117.
cluding if the other side violates the rules) over time is likely either to rupture in crisis or else simply have less and less purchase as universal rules.  

Although the Manual still talks gamely of reciprocity, it is doubtful that many American troops battling today’s depraved foes expect to be treated by them as international law would require. How then do commanders and their lawyers rationalize lawful behavior to the troops? Can fear of punishment alone do the job? Maybe in some cases, but reinforcing the idea of honor and chivalry, which implicitly call upon the individual to do the right thing even when the enemy is not, can be an important motivator in modern war.

I believe that this is how Haque’s insistent reference to morality, which I see as involving honor and chivalry, can best be productively operationalized. Although I continue to disagree with how he expresses it at times, his underlying concept (as I interpret it anyway) that morality “matters” is more than just a philosophical good, but also a practical necessity if we are to expect the troops to adhere to the law under circumstances of extreme stress in the face of an adversary who cruelly mocks the most basic principles of the law of war.

Translating morality, qua morality, into more secular references to honor and chivalry may be a way to broadly and effectively access the warfighter’s psychology that one wishes to animate towards law of war compliance.

V. JOURNALISTS

Whatever consternation was produced by any other part of the Manual, nothing resulted in more outcry from the Fourth Estate than its references to journalists, and to the possibility that circumstances exist where they might be considered spies or belligerents. In a breathless editorial—The Pentagon’s Dangerous Views on the Wartime Press—The New York Times typified criticism by claiming that the Manual would make the work of journalists “more dangerous, cumbersome and subject to censorship,” demanding that its provisions relating to the “treatment of journalists covering armed conflicts . . . should be repealed immediately.”

93. Id.  
94. See, e.g., DOD Manual, supra note 1, ¶ 3.6.  
While the Pentagon96 offered a strong defense of this part of the Manual, as did others,97 I found the Times’ deeply-flawed and at times nonsensical editorial to unintentionally demonstrate why the public has so little confidence in newspapers these days, particularly when compared to its confidence in the military.98 Indeed, Americans’ trust in the media generally remains at “historical lows.”99 Though the Times itself seems to struggle with why this may be,100 the truth is that this editorial is an example of why people rightly are skeptical of the media’s ability to get things right.

In this instance, the Manual lays out the various legal statuses that might attach to journalists by saying: “[i]n general, journalists are civilians. However, journalists may be members of the armed forces, persons authorized to accompany the armed forces, or unprivileged belligerents.”101 It emphasizes that journalists “are regarded as civilians; i.e., journalism does not constitute taking a direct part in hostilities such that such a person would be deprived of protection from being made the object of attack.”102 However,
it also acknowledges the inarguable truth that there are times when even journalists can lose their protection. Specifically, the Manual points out that:

Journalists and Spying. Reporting on military operations can be very similar to collecting intelligence or even spying. A journalist who acts as a spy may be subject to security measures and punished if captured. To avoid being mistaken for spies, journalists should act openly and with the permission of relevant authorities. Presenting identification documents, such as the identification card issued to authorized war correspondents or other appropriate identification, may help journalists avoid being mistaken as spies.\textsuperscript{103}

As I pointed out in an op-ed, The New York Times, Dangerously Uninformed, vs. the Military,\textsuperscript{104} the Times is apparently unaware that the Manual does little more than lay out what the Geneva Conventions and other legal authorities have provided for decades. For example, the Times' editors decry the fact that the Manual notes that when journalists relay to adversaries “information of immediate use in combat operations,” such real-time and direct support of enemy warfighting efforts might jeopardize the protected status journalists normally enjoy.\textsuperscript{105} This is nothing new. The International Committee of the Red Cross (ICRC) makes clear that journalists are protected like other civilians,\textsuperscript{106} but not “for such time as they take a direct part in hostilities”—language which is itself taken directly from the 1977 Protocol I to the Geneva Conventions.\textsuperscript{107}

So what would constitute direct participation for a journalist? The Times ridicules the Manual for having what it calls a “vaguely-worded standard” in this regard.\textsuperscript{108} Actually, the ICRC itself uses “transmitting tactical targeting

\begin{footnotes}
\item[103] Id., ¶ 4.24.4.
\item[105] The Pentagon’s Dangerous Views on the Wartime Press, supra note 95.
\item[107] Protocol I, supra note 27, art. 51(3).
\item[108] The Pentagon’s Dangerous Views on the Wartime Press, supra note 95.
\end{footnotes}
intelligence for a specific attack" as one example of direct participation.\textsuperscript{109} Put another way, the Manual's illustration virtually mirrors the substance of the ICRC's assessment—something the Times could have easily discovered if they had exercised a modicum of due diligence.

One has to wonder whether anyone (other than the Times' editors) really believes that journalists have some kind of unfettered right to broadcast to ISIS militants or whomever might be listening that, for example, a clandestine military operation to rescue human shields is about to get under-

The Times also obviously resents that anyone would even suggest that a journalist might be involved in spying. In truth, it is hardly a news flash\textsuperscript{110} that spies have long used the "journalist" sobriquet as a cover.\textsuperscript{111} In fact, in reporting the death in 2013 of Austin Goodrich, a former CBS reporter-spy, the Times itself admits that he was "far from the only journalist doubling as a secret agent" in the 1950s and 1960s.\textsuperscript{112} Is the Times really so naive to think that in today's world where adversaries are willing to bury children alive,\textsuperscript{113} they would be squeamish about using journalists as secret agents?

It is not hard to figure out why journalists could be effective spies. After all, international law defines spying as "when [someone] acting clandestinely or on false pretenses . . . obtains or endeavors to obtain information in the zone of operations of a belligerent . . . with the intention of communicating it to the hostile party."\textsuperscript{114} Is not a journalist someone who "obtains or endeavors to obtain information in the zone of operations"? For its part, the American Press Institute (API) defines journalism as "the activity of gathering, assessing, creating, and presenting news and infor-


\textsuperscript{111} Murray Seeger, Spies and Journalists: Taking a Look at Their Intersections, NIEMAN REPORTS (Sept. 11, 2009), http://niemanreports.org/articles/spies-and-journalists-taking-a-look-at-their-intersections/.

\textsuperscript{112} Bruce Weber, Austin Goodrich, Spy Who Posed as Journalist, Dies at 87, NEW YORK TIMES, July 15, 2015, at A15.

\textsuperscript{113} Stephanie Nebehay, supra note 91.

\textsuperscript{114} Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, art. 29, Oct. 18, 1907, 36 Stat. 2227, T.S. No. 539.
One need not be a military expert to realize that the API definition reflects much the same skill set as that of a military intelligence officer. In short, the Manual’s concern about journalists is hardly unreasonable.

The ICRC understands that it is a real possibility that a journalist might actually be an intelligence operative, and simply insists that a journalist so suspected must not be subject to arbitrary detention, and must be given a fair trial.116 The Manual is, of course, fully supportive of such humane treatment.

In addition, the Times’ editorial reveals a blissful ignorance about the impact of modern technologies on battlefield reporting. A new study by the Royal Danish Defense College regarding the “weaponization of social media” gives examples as to how today’s press reporting is being exploited by terrorist organizations in combat:

Internet (live streamed news reports on web-TV) and social network media (e.g., Journalists tweeting from crisis areas) are also being used by non-state actors without sophisticated Intelligence Surveillance and Reconnaissance (ISR) assets to conduct Bomb Damage Assessment (BDA) of, e.g., their rocket attacks.117

In other words, even the most well-meaning journalist might be inadvertently aiding the enemy. This illustrates that, yes, there are instances where it is necessary to temporarily restrain reporting—even by bona fide journalists. This is completely legal, and not just under international law: The U.S. Supreme Court has never found that the First Amendment entitles journalists or anyone else to communicate to the enemy real-time information it can readily use to fight U.S. troops.118

Why? The court has held that it is “obvious and unarguable” that “no governmental interest is more compelling than the security of the Nation.”119 Indeed, in the 2010 case of Holder v. Humanitarian Law Project, the court upheld as consistent with the First Amendment the actual criminaliza-

116. CIII Study, supra note 68, at 118.
tion of the conveyance of relatively benign and unclassified legal information to designated terrorist organizations.  

The Times also arrogates to itself the right to declare who is or is not a journalist. When a Pentagon official raised the example of the assassination of the Afghan military commander Ahmad Shah Massoud in September 2001 by assassins who posed as television journalists, the Times editors scoffed that “[t]hey were not, in fact, journalists.”  

In the real world, however, determining who is or is not a journalist is not an easy thing, especially given that anyone with access to a social media can describe him or herself as a “citizen journalist.” These are, we are told, private individuals who “do essentially what professional reporters do.”  

Accordingly, although the Times objects mightily to a journalist accreditation process, should any “citizen journalist” with a Twitter account be allowed to trample around a battlefield transmitting whatever sensitive military activity interests him or her? Furthermore, is not some vetting appropriate in light of the Massoud incident? Again, even a cursory examination of Additional Protocol I clearly shows that it contemplates that it will be a government—not the Times or any newspaper—that “attests” to a person’s “status as a journalist.”  

I concluded my op-ed by observing that the United States needs a fully informed, robust and courageous media, particularly during wartime. And it needs reporters on the battlefield who are willing to accurately represent the facts to the public. The press, however, cannot deem itself above the Constitution or the international law to which America has bound itself. Nor can it be insensitive to the needs of those this country sends in harms’ way. Denigrating the military simply because its Manual reflects the law as it exists is a formula for the further loss of confidence of the American people in their newspapers and other journalistic endeavors.

121. The Pentagon’s Dangerous Views on the Wartime Press, supra note 95.
123. Id.
124. Protocol I, supra note 27, art. 79(3).
VI. CYBER

One of the most interesting sections of the Manual (and not the first time about which this writer is commenting\(^{125}\)) is Chapter 16 on Cyber Operations. What is remarkable is not so much anything dramatically new in the text, but rather that it was included at all. For many years, almost everything about cyber, other than that which related to purely defensive cyber matters, was classified; indeed, the Pentagon’s joint doctrine was only declassified in 2014.\(^{126}\) What discussion of the U.S. view of law in this area that existed in official venues was mainly based on a long-available 1999 U.S. Department of Defense General Counsel (GC) memorandum,\(^{127}\) and the ground-breaking 2012 speech by Harold Koh, then legal advisor to the U.S. State Department.\(^{128}\)

The Manual’s chapter on cyber operations hews to the earlier DoD memo and the Koh speech in virtually all particulars. Controversy may exist, however, in at least two areas. Specifically, the Manual diverges a bit from what many scholars believe is the proverbial “gold” standard, the highly respected Tallinn Manual (which it does not even cite). An effort of international experts, under the auspices of NATO’s Cooperative Cyber Defence Centre of Excellence, the Tallinn Manual attempts to capture and interpret the extant international law applicable to cyber.\(^{129}\)

To be sure, the Manual and the Tallinn Manual are in accord in many respects,\(^{130}\) but the two documents part ways on the issue of the degree of


\(^{128}\) Harold Hongju Koh, Legal Advisor of the U.S. Dep’t of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.

\(^{129}\) THE TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBERWARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

force that is necessary to trigger the right of self-defense under Article 51 of the UN Charter. The Tallinn Manual takes the view of most international law scholars that the prohibition on the "use of force," found in Article 2(4) of the Charter, is different from what might constitute an "armed attack" under Article 51. The Manual, however, takes the position—as reflected in the Koh speech—"that the inherent right of self-defense potentially applies against any illegal use of force." Other scholars, like Schmitt, also seem to be acknowledging that significant cyber events may have an effect so severe that States will consider them the equivalent of an armed attack even in the absence of direct, physical destruction as is the case with more traditional weaponry, even though the boundaries may not be clear. Schmitt says that "[s]hutting down the national economy is probably an act of war, but short of that, we're not certain." Despite having been published since June of 2015, many pundits seem unaware of this chapter of the Manual. For example, in September of 2015, an op-ed appeared asserting that in cyber a "new battlefield has emerged

---


> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

132. Id., art. 2(4). That article provides: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

133. DOD Manual, supra note 1, ¶ 1.11.5.2, 16.3.3.1.

134. Id., ¶ 16.3.1 (citations omitted).


136. Id.
that has anonymous combatants, civilian targets and no established rules.\(^\text{137}\) Actually, as both the \textit{Manual} and the Tallinn Manual make clear, there are rules, but ascertaining the facts by which to apply those rules can be difficult in the cyber arena. Still, as Schmitt concedes, circumstances can arise where the legal answers are not yet clear.\(^\text{138}\) This is especially true regarding hostile cyber incidents below the threshold of “force,” so we can expect further developments in future editions of the \textit{Manual}.\(^\text{139}\)

Even more significant is a letter from several congressmen to the State Department insisting that “[n]ow is the time for the international community to seriously respond again with a binding set of international rules for cyberwarfare: an E-Neva Convention.\(^\text{140}\)

Perhaps the issue is that although the \textit{Manual} sketches out the DoD’s view of the law, it does not provide a “cookbook” setting out the legal status for every possible cyber incident. As Admiral Rogers pointed out in recent testimony, the DoD is still “still working [its] way through” what constitutes an “act of war” in a given situation.\(^\text{141}\) That is understandable, but even if the \textit{Manual} never becomes a cookbook (as it never should be), it should be amended as more detailed guidance becomes available. In this respect, the \textit{Manual} is more of a beginning, than a finished state of the U.S. view of the law of cyber operations.

\section{Conclusion}

This short article by no means examined all of the \textit{Manual}'s critiques, let alone all the thoughtful dialogue it engendered. For example, Army Reserve Major Patrick Walsh’s examination of the \textit{Manual} led him to make an

\begin{itemize}
\item \(^{138}\) Fairchild, \textit{supra} note 135 (quoting Michael Schmitt).
\end{itemize}
interesting call to correct what he terms as a "major flaw" in the Uniform Code of Military Justice as he believes it has "no provision for command responsibility." I am not sure I agree with him as Articles 18 and 21 of the Code do provide for courts-martial jurisdiction for violations of the "law of war," which would include offenses related to command responsibility.

Professor Jordan Paust points out that the Supreme Court has on more than one occasion concluded that Congress has included, in language very similar to that of the current Code, the authority to try offenses arising under the law of war. Accordingly, I think that with innovative charging, an appropriate law of war crime based on command responsibility can be pursued within the existing parameters of the Code.

Another interesting critique comes from the highly-respected law of war expert Professor Geoffrey Corn. Corn found it "perplexing" that the Manual did not elevate the LoW obligation "to take all feasible precautions to mitigate the risk to civilians" from a "mere rule" to "a fundamental principle" of the LoW. Candidly, it is not perplexing to me because while the Manual has shown some fresh thinking regarding precautions to be taken during attacks, it is still essentially a lex lata, as opposed to a lex ferenda, document. His proposal is just not reflective of the vast majority of interpretations of the LoW's fundamental principles. More specifically, it is hard to see how it might affect the actual practice of the LoW, except perhaps to obscure the point that it is "excessive" civilian casualties that the LoW focuses upon. In fact, in the current war against ISIS, credible reports


144. E-mail from Jordan Paust, Mike and Teresa Baker Law Center Professor of International Law at the Law Center of the University of Houston, to Charles J. Dunlap, Jr., Professor of the Practice of Law, Duke University School of Law (Oct. 16, 2015) (on file with the author). See also Jordan Paust, After My Lai: The Case for War Crime Jurisdiction Over Civilians in Federal District Courts, 50 TEXAS LAW REVIEW 6, 10–28 (1971).


146. See supra, sec. III.

147. See, e.g., Gary D. Solis, The LAW OF ARMED CONFLICT ch. 7 (2010) (defining the core principles of the law of armed conflict as distinction, military necessity, unnecessary suffering and proportionality).
about unwarranted caution about civilian casualties (that is, beyond what the LoW requires) "is sparking a crisis in confidence that has invited further violence emboldening others to take action not aligned with U.S. interests." 148

Nevertheless, these essays and others are the sort of thought-provoking dialogue one hopes the Manual will produce. They suggest that the Manual will likely become something of a "living" document. As already noted, by its own terms it solicits feedback, and explicitly preserves the idea that the views it contains will evolve. 149 As new weapons, new strategies and new adversaries emerge, we can—and should—expect to see just such an evolution. After all, as the Nuremberg Tribunal observed, the "law is not static, but by continual adaption follows the needs of a changing world." 150

Still, it remains to be seen the degree to which the Manual influences the development of the law of war. Professor Eric Jensen of Brigham Young Law School expresses concern that the Manual officially bills itself as merely providing "information on the law of war to DOD personnel responsible for implementing the law of war and executing military operations," instead of aggrandizing for itself a more directive mantle of definitive guidance. 151 He also seems displeased that the Manual states that it "does not necessarily reflect the views of any other department or agency of the U.S. Government or the views of the U.S. Government as a whole" as this may undermine its value as opinio juris. 152

While Jensen's criticisms are thoughtful and important, I think that the language that concerns him is simply bureaucratic conventions required to end the lengthy interagency coordination process that reportedly stalled the Manual's publication for so long. 153 I would expect that the Manual will rather quickly become considered the definitive statement of the United States on the LoW. Because the United States has so much practical experience in warfighting, and especially in the complex conflicts of the twenty-

148. Depta, supra note 43.
149. DoD Manual, supra note 1, ¶ 1.1.1 ("This manual does not, however, preclude the Department from subsequently changing its interpretation of the law.").
152. Id. (citing DoD Manual, supra note 1, ¶ 1.1.1).
153. See supra notes 5, 6 and accompanying text.
first century, I would be surprised if other nations do not also find it to be the most influential document of its genre.

Allow me to close by paraphrasing what I said about another law of war manual154 because I believe it to be equally (or more) applicable here:

Efforts like the drafting of the [DoD] Manual are but one part of the overall preparation for lawful, ethical combat. The [DoD] Manual can be instrumental not just to protecting the lives of innocent civilians, or even to defending the perquisites of states, per se. It can also help to provide a degree of confidence, if not comfort, to those who are asked by their nation to perform the most difficult of tasks under the most demanding of circumstances. For this, if nothing else, the enormous effort that produced the [DoD] Manual finds its justification.155

154. The Program on Humanitarian and Conflict Research at Harvard University, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2013).
Off Target: Selection, Precaution, and Proportionality in the DoD Manual

Adil Ahmad Haque

92 INT'L. L. STUD. 31 (2016)
Off Target:
Selection, Precaution, and
Proportionality in the DoD Manual

Adil Ahmad Haque*

CONTENTS

I. Introduction .................................................................................................................. 32
II. Target Selection .......................................................................................................... 36
   A. The Law ................................................................................................................... 37
   B. The Manual ............................................................................................................... 41
   C. Logic ......................................................................................................................... 45
III. Precautions in Attack and Acceptance of Risk ......................................................... 48
   A. The Law ................................................................................................................... 48
   B. The Manual ............................................................................................................... 52
   C. Logic ......................................................................................................................... 57
IV. Proportionality and Human Shields ........................................................................... 58
   A. The Law ................................................................................................................... 59
   B. The Manual ............................................................................................................... 63
   C. Responsibility ........................................................................................................... 72
      1. Law ......................................................................................................................... 72
      2. Logic ....................................................................................................................... 76
   D. Deterrence ............................................................................................................... 78
   E. Fairness ..................................................................................................................... 82
V. Conclusion ................................................................................................................... 83

* Professor of Law and Judge Jon O. Newman Scholar, Rutgers Law School.
The thoughts and opinions expressed are those of the author and not necessarily of
the U.S. government, the U.S. Department of the Navy or the U.S. Naval War College.
I. INTRODUCTION

According to its authors, the purpose of the United States Department of Defense (DoD) Law of War Manual “is to provide information on the law of war to DoD personnel responsible for implementing the law of war and executing military operations.”1 Unfortunately, the Manual provides misinformation on the law of war governing targeting and attack to its users and readers. Those who look to the Manual for guidance on these critical matters will be led astray.

Lawful targeting begins with lawful targets. Problems with the Manual begin there as well. I will mention three familiar problems before turning to my own concerns. First, international law protects civilians unless and for such time as they take a direct part in hostilities, through acts likely to directly cause harm in support of one party and against another.2 In contrast, the Manual asserts that it is lawful to target civilians who “effectively and substantially contribute to an adversary’s ability to conduct or sustain combat operations.”3 On the contrary, civilians do not lose their protection from attack through “acts that—although ‘ultimately harmful to the enemy’—are not part of military operations.”4 In addition, the Manual states that the lawfulness of attacking a civilian may depend on “whether the [civilian’s] act is of comparable or greater value to a party’s war effort than acts that are commonly regarded as taking a direct part in hostilities.”5 On the contrary, participation in a party’s war effort, no matter how valuable, is not legally equivalent to direct participation in hostilities.

2. See, e.g., Prosecutor v. Galić, Case No. IT-98-29-T, Judgment, ¶ 48 (Int’l Crim. Trib. for the former Yugoslavia Dec. 5, 2003); Prosecutor v. Rutaganda, Case No. ICTR-96-3-T, Judgment, ¶ 100 (Dec. 6, 1999); International Committee of the Red Cross, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law 46 (2009) [hereinafter Interpretive Guidance] (including acts that are an integral part of military operations likely to directly cause harm).
3. DoD Manual, supra note 1, ¶ 5.9.3. The Manual illustrates its position with the example of Vietnamese villagers “of all ages and sexes [who], willingly or under duress, served as porters [for] . . . communist forces.” Id. ¶ 5.9.3 n.227. It seems that, according to the Manual, children forced to serve as porters for opposing forces are lawful targets.
5. DoD Manual, supra note 1, ¶ 5.9.3.
Second, under international law, an object is a military objective liable to lawful attack only if it makes “an effective contribution to military action.”\(^6\) In contrast, the *Manual* states that it is lawful to attack any object that makes “an effective contribution to the war-fighting or war-sustaining capability of an opposing force.”\(^7\) On the contrary, as Dinstein writes, “[t]he ‘war-fighting’ limb can pass muster, . . . but the ‘war-sustaining’ limb is untenable. . . . For an object to qualify as a military objective, there must exist a proximate nexus to ‘war-fighting’.”\(^8\)

Finally, the *Manual* states that “[u]nder customary international law, no legal presumption of civilian status exists for persons or objects, nor is there any rule inhibiting commanders or other military personnel from acting based on the information available to him or her in doubtful cases.”\(^9\) On the contrary, such a legal rule exists under customary international law, though its precise contours remain unsettled. According to one distinguished group of experts, “[t]he degree of doubt necessary to preclude an attack is that which would cause a reasonable attacker in the same or similar circumstances to abstain from ordering or executing an attack.”\(^10\) Alternatively, the degree of doubt necessary to preclude an attack may vary based on, “inter alia, the intelligence available to the decision maker, the urgency of the situation, and the harm likely to result to the operating forces or to persons and objects protected against direct attack from an erroneous decision.”\(^11\) By denying that any such legal rule exists, the *Manual* misses an opportunity to contribute to the progressive development of its content.\(^12\)

This article focuses on three elements of lawful targeting that are less frequently discussed, but on which the lives of civilians often depend: tar-
get selection, precautions in attack, and proportionality. The Manual says that

AP I provides that "[w]hen a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects." The United States has expressed the view that this rule is not a requirement of customary international law.\(^3\)

According to this passage, attackers presented with a choice of targets for obtaining a similar military advantage have no legal obligation to select the target that places the fewest civilians in danger. In addition, in its discussion of precautions in attack, the Manual says that

if a commander determines that taking a precaution would result in operational risk (i.e., a risk of failing to accomplish the mission) or an increased risk of harm to their own forces, then the precaution would not be feasible and would not be required.\(^4\)

According to this passage, attackers have no legal obligation to take precautions that will entirely avoid or greatly reduce risk to civilians if doing so would involve any additional risk to themselves or to their mission. Most dramatically, in its section on proportionality, the Manual says that

Harm to the following categories of persons and objects would be understood not to prohibit attacks under the proportionality rule: (1) military objectives [that is, enemy combatants, civilians taking a direct part in hostilities, and military equipment]; (2) certain categories of individuals who may be employed in or on military objectives; and (3) human shields.\(^5\)

According to this passage, the proportionality rule permits attackers to collaterally kill civilians forced to serve as human shields, no matter how many, in pursuit of any military advantage, no matter how small.

Of course, it is possible that these passages simply misstate DoD's legal positions. If so, then perhaps this article will encourage their prompt revision. However, after nearly two decades of drafting and inter-agency re-

\(^{13}\text{DOD Manual, supra note 1, ¶ 5.11.5.}\)
\(^{14}\text{Id. ¶ 5.3.3.2.}\)
\(^{15}\text{Id. ¶ 5.12.3.}\)
view, we should presume that the Manual means what it says. Certainly, we should not presume that DoD expects users of the Manual to read between its lines to divine its true meaning. After all, it is a manual, not a constitution, we are expounding.

On each point, the Manual reflects neither lex lata nor lex ferenda. In my judgment, the Manual does not describe customary international law as it was in 1996, when work on the Manual began. Certainly, the Manual does not describe customary international law as it is in 2016. State practice, including U.S. practice, continued to evolve in the intervening decades. The Manual “is intended to be a description of the law as of the date of the manual’s promulgation.”16 In my view, the Manual describes a law of war that no longer exists.

The law of war—also known as the law of armed conflict (LOAC) or international humanitarian law (IHL)—aims to strike a reasonable balance between humanity and military necessity. Yet, on these critical issues, the Manual does not merely tip the balance in favor of attackers. Instead, the Manual effectively strikes civilians from the scales. The balance itself is often misunderstood. Legal positions that ignore civilian protection frequently reduce rather than enhance military effectiveness. If the law of war loses its moral credibility then combatants will not trust that they can obey lawful orders in good conscience. They will hesitate, question, and dissent, looking elsewhere for the normative guidance that law ought to provide. Instead of relying on the law to strike a reasonable balance between humanity and necessity, combatants will have no choice but to strike their own.17

My substantive objections to the Manual should not be mistaken for personal criticism of its authors. The authors of the Manual are fine people, good lawyers, and dedicated public servants. They operated under a variety of institutional constraints, including the need to reach consensus and to reflect prior DoD positions. Nevertheless, the stakes are too high to mince words. With all due respect to its authors, the positions taken in the Manual are both wrong and dangerous. If U.S. forces do what the Manual permits then they will kill civilian men, women, and children in violation of interna-

17. Cf. Richard C. Schragger, Cooler Heads: The Difference between the President’s Lawyers and the Military’s, SLATE (Sept. 20, 2006), http://www.slate.com/articles/news_and_politics/jurisprudence/2006/09/cooler_heads.html ("Law allows our troops to engage in forceful, violent acts with relatively little hesitation or moral qualms. Law makes just wars possible by creating a well-defined legal space within which individual soldiers can act without resorting to their own personal moral codes.").
tional law and without moral justification. On the other hand, if U.S. forces refrain from conduct that the Manual claims is lawful then the actual conduct of war will be regulated not by international law but by personal conscience and national policy. Either outcome subverts the aim of protecting civilians and guiding soldiers through international legal norms.

The law of war is international law. The law for the United States is the law for Russia and China, for Saudi Arabia and Sri Lanka, for North Korea and Pakistan, for Syria and Sudan. The legal authority that we claim for ourselves today, others will claim for themselves tomorrow. It is no defense of the Manual that our armed forces, surely, will never actually do what the Manual says that they may lawfully do. Surely, their moral character, professional integrity, and martial honor will prevent them from exercising the outer limits of the legal authority that the Manual claims for them. Yet what the Manual claims is legal for us, the Manual necessarily claims is legal for all.

The organization of this article is straightforward. Each part opens with a scenario that illustrates the legal issue at hand, followed by a presentation of contemporary international law and a legal analysis of the Manual’s contrary position as well as its supporting evidence. The first two parts—on target selection and precautions in attack—conclude by examining the logic of the Manual’s position, or lack thereof. In contrast, the final part—on proportionality and human shields—concludes by assessing three rather cursory arguments that the Manual offers in support of its position. Since these arguments raise quite distinct issues, I analyze them separately, challenging their bases in law and logic.

II. TARGET SELECTION

Opposing forces need to cross both Bridge A and Bridge B in order to transport weapons and equipment to the front line. Destroying either bridge would prevent them from doing so. Bridge A is a major commuter route, while Bridge B carries little civilian traffic. If your forces destroy Bridge A then—even if your forces take reasonable precautions in carrying out the attack—you expect them to kill at least ten civilians. In contrast, if your forces destroy Bridge B then you expect them to kill no civilians. You determine that the deaths of ten innocent civilians, though tragic, would not be excessive in relation to the anticipated military advantage of destroying Bridge A. Of course, you could obtain a similar military advantage without killing any civilians, simply by destroying Bridge B instead.
As a legal officer, what would you advise? As a commander, what would you order? As an operator, what order would you obey?

A. The Law

Under Protocol I,

[when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.]

This provision—which I will call the target selection rule—was adopted unanimously and ratified by all 174 States party to Protocol I without reservation. Applied to the scenario described above, under Protocol I it would be unlawful to destroy Bridge A, killing ten civilians, rather than destroy Bridge B, killing no civilians, to obtain a similar military advantage. Equivalent scenarios may arise involving roads, tunnels, railroads, power lines, and other lines of communication. In such cases, the target selection rule simply requires what common sense and elementary considerations of humanity demand.

Of course, the United States is one of nineteen States that are not party to Protocol I. Accordingly, the United States is bound only by customary international law. Some argue that, paradoxically, the near-universal ratification of a treaty occludes its relationship with customary law. On this approach, apparently positive practice of State parties like Australia, Germany, and the United Kingdom may be dismissed as reflecting treaty obligations. Conversely, the wartime conduct of non-parties like Sri Lanka may be accepted as contrary practice that reflects or changes customary law. Indeed, if we exclude the practice of 174 States and consider only the prac-


19. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, supra note 6, at 65.

20. According to the so-called “Baxter paradox,” “as the number of parties to a treaty increases, it becomes more difficult to demonstrate what is the state of customary international law dehors the treaty.” In addition, “[a]s the express acceptance of the treaty increases, the number of states not parties whose practice is relevant diminishes. There will be less scope for the development of international law dehors the treaty . . . .” See Richard Baxter, TREATIES AND CUSTOM, 129 RECUEIL DES COURS 64, 73 (1970).
tice of nineteen States then it is hard to see how any constraint on the con-
duct of hostilities could reflect the extensive and virtually uniform State
practice necessary to establish customary law. In my view, this approach is
a blueprint for legal stagnation at best and legal regression at worst.

Fortunately, the relationship between treaty and custom is not so para-
doxical. A treaty provision may codify established customary law, crystalize
emerging customary law, or inspire the progressive development of cus-
tomary law. The fact that no party to Protocol I introduced objections,
declarations or reservations regarding the target selection rule is itself sub-
stantial—though not dispositive—evidence that many parties believed that
the target selection rule either codified existing custom or crystallized
emerging custom.

According to the ICRC, the target selection rule,

described “as the lesser of two evils,” was already in the Draft Rules of
1956 (Article 8(a), paragraph 2). It was included in the 1973 draft and the
Conference accepted it without much discussion. It is in accordance with
the actual practices of belligerents in certain cases, particularly with re-
spect to occupied allied countries.

In this field mention could be made of attacks launched against enemy
road and rail traffic; some belligerents have tried to attack the adversary
only when this would not result in severe damage for the population. In-
stead of attacking railway stations, which are usually located in towns, the
railway lines were hit at crucial points, but away from inhabited areas; the
same action was taken with respect to roads.

Such examples show that it is possible to choose objectives so that their
destruction does not imperil the population and civilian objects, while still
gaining the same military advantage.

(Feb. 20). See also Hon. Fausto Pocar, To What Extent Is Protocol I Customary International
Law?, 78 INTERNATIONAL LAW STUDIES 337, 341 (2002) (noting that “the treaty itself is
an important piece of State practice for the determination of customary law, although its
role in this regard must be carefully assessed,” and considering “the impact that any sub-
sequent practice of the contracting States in the application of the treaty which establishes
their agreement or disagreement regarding its interpretation may bear on the development
of a customary norm”).

22. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GE-
NEVA CONVENTIONS OF 12 AUGUST 1949, ¶¶ 2226–28 (Yves Sandoz, Christophe Swinarski
& Bruno Zimmermann eds., 1987) [hereinafter PROTOCOL I COMMENTARY].
Evidently, no party felt that the target selection rule places unreasonable constraints on military operations. To my knowledge, no party has expressed regrets in the decades since.

For its part, the U.S. Air Force endorsed the target selection rule in its 1976 law of war pamphlet—one year prior to Protocol I’s adoption and two years prior its entry into force.23 Logically, the Air Force must have thought that the proposed treaty provision codified established customary law or that the negotiating process was crystallizing emerging customary law. Certainly, the Air Force could not have thought that the target selection rule was legally binding on U.S. forces in virtue of a treaty that had not been finalized let alone ratified by the United States.

Subsequent State practice and _opinio juris_ confirms that the target selection rule is a requirement of customary international law.24 The ICRC cites the “official statements and reported practice” of thirteen States directly affirming the customary status of the rule.25 Importandy, the ICRC cites the practice of seven States that were not, at the time, parties to Protocol I and whose positive practice therefore cannot be attributed to their treaty obligations.26 Finally, the ICRC “found no official contrary practice” denying that the target selection rule is customary law. The ICRC found “only one instance of apparently contrary practice,” to which we will return shortly.

Unsurprisingly, the target selection rule is found in the law of war manuals of at least eighteen States, including Australia, Canada, France, Italy, Spain, Sweden, and the United Kingdom.27 Although most of these States are party to Protocol I, it is hard to believe that, were they to with-

23. Department of the Air Force, AFP 110-31, International Law—The Conduct of Armed Conflict and Air Operations 5-9–5-10 (1976). _See also id. at 5-7_ (“Based on these developments [including the preparation of Protocol I] it is now possible to discuss meaningfully the law of armed conflict as it affects aerial bombardment.”). The 1976 pamphlet was subsequently rescinded but remains widely cited as evidence of U.S. practice, including in the DoD Manual itself.

24. _CUSTOMARY INTERNATIONAL HUMANITARIAN LAW_, _supra_ note 6, at 65 (“State practice establishes this [target selection] rule as a norm of customary international law applicable in international, and arguably also in non-international, armed conflicts.”).

25. _Id_. These States are Egypt, France, Jordan, Indonesia, Iran, Iraq, Israel, Kenya, Malaysia, the Netherlands, Syria, the United States (more on this in a moment), and Zimbabwe.

26. _Id. at 66–67_. These States are France, Indonesia, Iran, Israel, Kenya, Malaysia, and the United States (again, more on this in a moment).

27. _Id. at 65._
draw from Protocol I, these States would consider themselves legally free to ignore alternative targets that offer similar military advantage but risk less civilian harm.

Tellingly, the target selection rule appears in nine military manuals applicable to non-international armed conflicts, as well as in agreements between parties to the (partly) non-international conflict in the former Yugoslavia. This practice also cannot be attributed to obligations found in Protocol I, since the Protocol applies only to international armed conflicts. Again, the absence of contrary practice is striking. No party to Protocol I has denied that the target selection rule applies to non-international armed conflicts. For their part, the expert drafters of the well-regarded San Remo Manual on the Law of Non-International Armed Conflict also concluded that the target selection rule is part of customary law applicable to non-international armed conflict.

Likewise, the International Criminal Tribunal for the former Yugoslavia (ICTY) found that the provisions of Article 57 of Protocol I, which include the target selection rule, “are now part of customary international law, not only because they specify and flesh out general pre-existing norms, but also because they do not appear to be contested by any State, including those which have not ratified the Protocol.” In particular, the ICTY stated that these provisions spell out the “general principle prescribing that reasonable care must be taken in attacking military objectives so that civilians are not needlessly injured through carelessness.”

Finally, the well-regarded HPCR Manual on International Law Applicable to Air and Missile Warfare endorses the target selection rule as a “black-letter

---


31. Id.
rule” of customary international law. The HPCR Manual reflects the consensus views of a 31-member group of experts from Australia, Canada, China, Germany, Israel, Norway, the UK, and the United States, among other nations. According to the Commentary on the HPCR Manual,

Whenever three or more participants in the Group of Experts objected to a given text, it was changed to meet such objections or bridge over conflicting views. In the rare instances in which compromise formulas proved beyond the reach of the Group of Experts, it was agreed to follow in the text the majority view but to give in the Commentary full exposure to the dissenting opinions.

Tellingly, the text of the HPCR Manual restates the target selection rule without qualification and the Commentary records no dissenting opinions regarding the rule’s customary status.

B. The Manual

As we have seen, the U.S. Air Force endorsed the target selection rule in its 1976 law of war pamphlet, which can only be interpreted as an acceptance of the rule as a requirement of customary international law. Nevertheless, the DoD Manual states the following:

AP I provides that “[w]hen a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.” The United States has expressed the view that this rule is not a requirement of customary international law.

It follows that, according to the Manual, States that are not party to Protocol I are not bound by the target selection rule. Returning to the example with which this part began, the Manual entails that you may lawfully strike

---

32. COMMENTARY ON THE HPCR MANUAL, supra note 10, at 128.
33. Interestingly, the group of experts included W. Hays Parks of the DoD’s Office of General Counsel. Id. at 9. If Parks conveyed the DoD’s position on this issue then it appears that it did not garner much support from other members of the group.
34. Id. at 4.
35. AFP 110-31, supra note 23, at 5-9–5-10.
36. DOD MANUAL, supra note 1, ¶ 5.11.5.
either Bridge A, killing ten civilians, or Bridge B, killing no civilians. Of course, you must take feasible precautions in attacking either target and cancel or suspend an attack on either target if the expected harm to civilians appears excessive in relation to the anticipated military advantage. However, according to the Manual, if an attack on either target would satisfy these requirements then the choice between the two is not governed by any legal rule. So far as the law is concerned, you may select your target by flipping a coin rather than by considering the likely consequences for civilians.

Importantly, the Manual does not say that the target selection rule of API is a requirement of customary international law provided that it is interpreted in some specified way. On the contrary, the Manual says that the target selection rule of API is not a requirement of customary international law. Nor does the Manual identify an alternative rule of customary law regulating the selection of targets that promise similar military benefits but threaten different humanitarian costs. It seems that, according to the Manual, customary law is silent on this basic element of warfare.

Strikingly, the Manual does not cite the practice or opinio juris of a single foreign State in support of its position that the target selection rule is not a requirement of customary international law. Nor does the Manual reflect U.S. operational practice. The Manual does not cite a single occasion on which U.S. forces were faced with a choice of targets for obtaining similar military advantage, knowingly selected a target that put more civilians in harm’s way than other targets, and later claimed that their selection of targets conformed to customary law. Indeed, it is hard to imagine a U.S. commander ordering an attack under such circumstances or to imagine a U.S. operator obeying such an order.

Instead, the Manual quotes a 1991 telegram sent by the United States to the ICRC in response to an ICRC memorandum on the applicability of international humanitarian law in the Gulf region:

Paragraph 4B(4) [of the ICRC memo] contains the language of Article 57(3) of Protocol I, and is not a part of customary law. The provision applies “when a choice is possible . . . ;” it is not mandatory. An attacker may comply with it if it is possible to do so, subject to mission accomplishment and allowable risk, or he may determine that it is impossible to make such a determination.37

37. Id. ¶ 5.11.5 n.303 (quoting U.S. Comments on the International Committee of the Red Cross’s Memorandum on the Applicability of International Humanitarian Law in the
Like the *Manual*, the telegram did not cite the practice or *opinio juris* of a single foreign State in support of its position that Article 57(3) of Protocol I is not a part of customary law. Perhaps the authors of the *Manual* felt institutionally constrained to restate the position taken in the telegram. Alternatively, perhaps the authors were well-positioned to encourage a change in U.S. policy. In any event, the *Manual* can find no legal support in a bare assertion that, even if tenable in 1991, is unsustainable in 2016.

For its part, the ICRC initially seemed puzzled by the telegram, writing that “the United States denied that this rule was customary but then restated the rule and recognised its validity, consistent with its other practice,” namely the 1976 Air Force pamphlet. The ICRC ultimately interpreted the telegram not as a rejection of the rule but as a qualified endorsement of it, writing that:

The United States has emphasised that the obligation to select an objective the attack on which may be expected to cause the least danger to civilian lives and to civilian objects is not an absolute obligation, as it only applies “when a choice is possible” and thus “an attacker may comply with it if it is possible to do so, subject to mission accomplishment and allowable risk, or he may determine that it is impossible to make such a determination.”

Of course, the *Manual* cites the telegram for the proposition that “[t]he United States has expressed the view that this rule is not a requirement of customary international law.” It therefore seems that the *Manual* rejects the ICRC’s interpretation of the telegram and that the citation to the telegram does not in any way qualify the denial that the target selection rule is a rule of customary law.

---


38. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, supra note 6, at 67.

39. *Id.*

In fact, the telegram nowhere recognizes the validity of the target selection rule as a part of customary law. The first sentence says that Article 57(3) "is not a part of customary law." The second and third sentences state the U.S. interpretation of "[t]he provision"—that is, of Article 57(3)—specifically of the phrase "when a choice is possible." However, since the United States is not a party to Protocol I, Article 57(3) does not apply to the United States no matter how it is reasonably interpreted.  

Perhaps the ICRC was confused by the telegram’s repeated use of the pronoun "it." However, upon close inspection, "it" clearly refers to "the provision," which in turn refers to Article 57(3) of Protocol I, which the telegram clearly says is not a part of customary law. The telegram does not say that Article 57(3) imperfectly reflects customary law. The telegram says that Article 57(3) is not a part of customary law.

In any event, if the Manual’s authors intended the provision to be a qualified endorsement of the target selection rule as a requirement of customary international law, then they would have made that clear in the text of the Manual. They would not have done so through a parenthetical quotation contained in a footnote that denies that the rule is part of customary law. In my judgment, the Manual is clearly wrong, but at least it is wrong clearly.

By way of contrast, the HPCR Manual recognizes the target selection rule as a requirement of customary international law. The Commentary to the HPCR Manual goes on to state that

There is no requirement to select among several objectives if doing so would be militarily unreasonable. As an example, if a choice has to be made between two alternative military objectives—one of which is more densely defended than the other—the attacker is not required to select the latter when heavy casualties are anticipated to the attacking force.  

41. It may seem odd for the United States to offer an interpretation of a treaty provision to which it is not bound and which it does not recognize as reflecting customary law. In fact, the United States routinely comments on the interpretation of Protocol I, including in the Manual itself. See, e.g., DoD Manual, supra note 1, ¶ 5.3.3.4 ("AP I Obligation to Take Constant Care to Spare Civilians and Civilian Objects"); id. ¶ 5.5.3.2 ("AP I Presumptions in Favor of Civilian Status in Conducting Attacks"); id. ¶ 5.5.8.2 ("AP I Obligation for Combatants to Distinguish Themselves During Attacks or Military Operations Preparatory to an Attack"); id. ¶ 5.9.1.2 ("AP I, Article 51(3) Provision on Direct Participation in Hostilities").

42. Commentary on the HPCR Manual, supra note 10, at 129.
The authors of the HPCR Manual had no trouble clearly endorsing the target selection rule as part of customary law while explaining how they interpret it. If the drafters of the DoD Manual had wished to do the same then they were more than capable of doing so.

The United States now appears to stand alone as the only nation in the world to deny that the target selection rule is a requirement of customary international law. The United States has yet to offer any evidence in support of its claim, other than its own twenty-five year old assertion. This bare assertion was itself unsupported by any recorded practice of acting contrary to the target selection rule and claiming legal authority to do so. Nor has the United States identified an alternative rule of customary law regulating the target selection process.

To be sure, States make customary international law. However, one State cannot make customary international law. When one State denies that a given rule is part of customary law that State must support its claim by citing foreign State practice and opinio juris, just like anyone else making an objective claim about the current state of customary law. In contrast, if a State cannot cite any contrary practice or opinio juris other than its own then it should concede that the rule otherwise reflects customary international law but argue that “the rule is not binding upon a State that has persistently objected to that rule during its development.”

In this case, the 1976 Air Force pamphlet endorsing the target selection rule makes it hard for the United States to persuasively argue that it has persistently objected to the rule and therefore is not bound by it. Nevertheless, such an alternative position would at least have some legal basis, since the Air Force pamphlet may have reflected the views of the Air Force but not that of the United States government as a whole. In contrast, the position of the Manual appears to have no legal basis.

C. Logic

In principle, positive law can be as illogical, immoral, or unwise as its human creators. However, we should reject an interpretation of positive law that generates illogical, immoral, or unwise results absent overwhelming evidence in its favor. As it happens, the Manual's rejection of the target se-

43. DoD Manual, supra note 1, ¶ 1.8.4 ("Even if a rule otherwise reflects customary international law, the rule is not binding upon a State that has persistently objected to that rule during its development.").
lection rule seems illogical given the Manual's recognition of the precautions rule, the proportionality rule, and the principle of humanity.\textsuperscript{44} To its credit, the Manual states that “[c]ombatants must take feasible precautions in conducting attacks to reduce the risk of harm to civilians.”\textsuperscript{45} In contrast, as we have seen, the Manual states that combatants need not select targets for attack so as to reduce the risk of harm to civilians. Evidently, harm to civilians often turns more on which targets are attacked than on how attacks on those targets are carried out. It seems illogical to regulate the latter but not the former.

Similarly, the Manual states that, when “the use of certain weapons rather than others may lower the risk of incidental harm, while offering the same or superior military advantage,” combatants are legally required to select the less risky weapons.\textsuperscript{46} In other words, according to the Manual, combatants must select weapons that lower the risk of incidental harm but need not select targets that do the same. Since the risk of incidental harm often depends more on the selection of targets than on the selection of weapons, again it seems illogical to regulate the latter but not the former.

In addition, the Manual accepts the proportionality rule, namely that “[c]ombatants must refrain from attacks in which the expected loss of life or injury to civilians . . . would be excessive in relation to the concrete and direct military advantage expected to be gained.”\textsuperscript{47} It is indeed wrong to kill civilians in pursuit of a military advantage too small to justify their deaths. However, it seems even worse to kill civilians in pursuit of a military advantage when one could obtain the same or a similar military advantage while killing fewer civilians. To refrain from the former but not the latter gets things backwards.\textsuperscript{48}

The target selection rule, the precautions rule, and the proportionality rule form a logically coherent triad. One rule governs what to attack, another governs how to attack, and the third governs whether to attack. Together, these three rules ensure that a lawful attack on a lawful target will inflict neither unnecessary nor excessive incidental harm on civilians. Rejecting

\textsuperscript{44} See infra.
\textsuperscript{45} DOD Manual, supra note 1, ¶ 5.11 (emphasis added).
\textsuperscript{46} Id. ¶ 5.11.3.
\textsuperscript{47} Id. ¶ 5.12.
\textsuperscript{48} Interestingly, the Canadian LOAC Manual states the target selection rule under the heading of “Proportionality and multiple targets.” CHIEF OF THE GENERAL STAFF (CANADA), B-GJ-005-104/FP-021, LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS ¶ 414 (2001).
one of these rules while endorsing the others leaves a logically inexplicable gap in the law.

The Manual’s rejection of the target selection rule seems even more illogical given that the rule appears to follow logically from a general principle that the Manual recognizes as foundational. The Manual accepts that the principle of humanity “forbids the infliction of suffering, injury, or destruction unnecessary to accomplish a legitimate military purpose.” Yet if an attacker can obtain the same military advantage by attacking any one of several targets then failing to select the target that places the fewest civilians in harm’s way inflicts more harm than necessary to accomplish that military purpose. For example, if you can obtain the same military advantage by destroying Bridge A, killing ten civilians, or by destroying Bridge B, killing no civilians, then an attack on Bridge A would seem to inflict suffering and injury unnecessary to accomplish a legitimate military purpose. In such cases, the target selection rule simply requires what the principle of humanity demands.

It seems illogical to recognize humanity as a fundamental principle of customary international law while insisting that the target selection rule is not a requirement of customary international law at all. In general, “[w]here a rule of customary international law is logical, because it can be deduced from an existing underlying principle, the burden of proving the rule by way of inductive reasoning is proportionally diminished.” Conversely, the burden of disproving a logical rule, deducible from an accepted principle, is proportionally increased. If the Manual offered decisive evidence of State practice and opinio juris in support of its position then we would have no choice but to accept that the fault lies not in the Manual but in the law itself. As we have seen, the Manual offers no such evidence, nor could it do so. In my view, the target selection rule was a requirement of customary international law when Protocol I was adopted in 1977, when the U.S. telegram to the ICRC was sent in 1991, and when work on the Manual began in 1996. Certainly, the target selection rule is a requirement of customary international law in 2016.

49. DOD Manual, supra note 1, ¶ 2.3.
III. PRECAUTIONS IN ATTACK AND ACCEPTANCE OF RISK

Based on surveillance, human intelligence, and thermal imagining, you determine that an insurgent commander is asleep in his home with his five young children. Based on the available information, you determine that a missile strike on the house will certainly kill the commander, as well as all five children, at no risk to your forces. You also determine that a night raid by special forces will almost certainly kill the commander and kill none of the children, but that there is a small chance that the commander will wake up and harm one of your operators before he is killed. Finally, you determine that the deaths of five innocent children, though horrific, would not be excessive in relation to the military advantage anticipated from killing the commander. Importantly, you could almost certainly obtain the same military advantage without killing any of the children by accepting a small risk to your own forces.

As a legal officer, what would you advise? As a commander, what would you order? As an operator, what order would you respect?

A. The Law

Under customary international law, “[a]ll feasible precautions must be taken to avoid, and in any event to minimise, incidental loss of civilian life, injury to civilians and damage to civilian objects.”51 This general rule of precautions in attack generates a number of specific obligations. Attacking forces must “do everything feasible to verify that targets are military objectives” in order to avoid mistakenly targeting civilians.52 Similarly, attacking forces “must do everything feasible to assess whether the attack may be expected” to inflict excessive harm on civilians.53 More distinctively, attacking forces “must take all feasible precautions in the choice of means and methods of warfare with a view to avoiding, and in any event to minimising, incidental loss of civilian life, injury to civilians and damage to civilian objects.”54 In particular, attacking forces “must give effective advance

51. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, supra note 6, at 51.
52. Id. at 55. See also Protocol I, supra note 18, art. 57(2)(a) (emphasis added).
53. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, supra note 6, at 58.
54. Id. at 56. See also Protocol I, supra note 18, art. 57(2)(a)(ii); id. art. 57(4) (“In the conduct of military operations at sea or in the air, each Party to the conflict shall . . . take all reasonable precautions to avoid losses of civilian lives and damage to civilian objects.”).
warning of attacks which may affect the civilian population, unless circumstances do not permit."\footnote{55}

Since no one disputes the customary status of the precautions rule, let us turn to its proper interpretation. Under customary international law, feasible precautions are those precautions that are "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations."\footnote{56} Intuitively, taking into account humanitarian and military considerations means balancing the humanitarian considerations in favor of taking a precaution and the military considerations against taking that precaution.\footnote{57} If the humanitarian considerations outweigh the military considerations then the precaution is required. Conversely, if the military considerations outweigh the humanitarian considerations then the precaution is not required.

Returning to the scenario with which this part began, the precautions rule would require you to raid the home, at some risk to your own forces, rather than to bomb the home, certainly killing the five children. In ordinary life, it is not reasonable to take a grave risk of killing innocent people rather than accept a small risk to yourself. The reasonable conduct of war is no different. While combatants are not always required to accept significant risks in order to protect civilians from others, combatants are required to accept some risks in order to avoid killing civilians themselves.\footnote{58}

This balanced approach is reflected in State practice, opinio juris and expert opinion. Since there is no difference between customary law and Protocol I with respect to precautionary obligations, let us examine the position of the United Kingdom. The UK \textit{Manual of the Law of Armed Conflict} notes that, in order to comply with their precautionary obligation to do everything feasible to verify that their targets are military objectives, "traditionally commanders have accepted some risk in identifying targets by using, for example, artillery spotters, forward air controllers, and intelligence gatherers operating in enemy-held territory."\footnote{59} In other words, attackers

\footnote{55} \textit{Customary International Humanitarian Law}, supra note 6, at 62. \textit{See also} Protocol I, supra note 18, art. 57(2)(c).

\footnote{56} \textit{Customary International Humanitarian Law}, supra note 6, at 54, 70.


\footnote{58} \textit{See}, e.g., Haque, supra note 12, at 106–10; David Luban, \textit{Risk Taking and Force Protection, in Reading Walzer} 277 (Yitzhak Benbaji & Naomi Sussman eds., 2014).

customarily accept risks to themselves if necessary to reduce the risk of mistakenly targeting civilians.

Elsewhere, the UK Manual observes that “[s]ometimes a method of attack that would minimize the risk to civilians may involve increased risk to the attacking forces. The law is not clear as to the degree of risk that the attacker must accept.”\textsuperscript{60} Put the other way around, attackers must accept some degree of risk in order to minimize risk to civilians, although the required degree of risk cannot be precisely quantified. Here, as elsewhere, the balance of humanitarian and military considerations calls for human judgment rather than mathematical calculation.

In a difficult passage that requires close reading, the UK Manual correctly notes that “[t]he proportionality principle does not itself require the attacker to accept increased risk,”\textsuperscript{61} but only to refrain from inflicting excessive incidental harm on civilians. In contrast, invoking the language of the precautions rule, the UK Manual goes on to say that if “alternative, practically possible methods of attack would reduce the collateral risks” then “the attacker may have to accept the increased risk as being the only way of pursuing an attack in a proportionate way.”\textsuperscript{62}

Obviously, attackers may have to accept increased risk if necessary to reduce the risk of inflicting excessive incidental harm on civilians. However, the phrase “pursuing an attack in a proportionate way” refers to how an attack should be carried out rather than to whether an attack should be carried out. In context, “pursuing an attack in a proportionate way” can only mean using methods of attack that reduce collateral risks without placing attackers at excessive or disproportionate risk.

To see this last point more clearly, notice that the UK Manual seems to adopt the view of A.P.V. Rogers, who writes that,

by adopting a method of attack that would reduce incidental damage, the risk to the attacking troops may be increased. The law is not clear as to the degree of care required of the attacker and the degree of risk that he must be prepared to take.\textsuperscript{63}

\textsuperscript{60} Id. ¶ 2.7.1.
\textsuperscript{61} Id.
\textsuperscript{62} Id.
\textsuperscript{63} A.P.V. Rogers, Zero-casualty Warfare, 82 INTERNATIONAL REVIEW OF THE RED CROSS 165, 177 (2000).
Importantly, Rogers concludes that “[m]ilitary necessity cannot always override humanity. In taking care to protect civilians, soldiers must accept some element of risk to themselves.” Rogers quotes the British Defense Doctrine of his day, which stated that “there may be occasions when a commander will have to accept a higher level of risk to his own forces in order to avoid or reduce collateral damage to the enemy’s civil population.” Elsewhere, Rogers warns that “the feasible test must not be restricted so far as to render nugatory the protection of the civilian population.”

Other experts share Rogers’ balanced view of precautions in attack. For example, as Michael Schmitt argues, “[i]t is reasonable to require military forces to assume some degree of risk to avoid collateral damage and incidental injury. They do so regularly. By this analysis, the greater the anticipated collateral damage or incidental injury, the greater the risk they can reasonably be asked to shoulder.” Similarly, Dinstein concludes that “[w]hat is called for is a reasonable ‘allocation of risk’ between the attacker’s military personnel and the enemy civilians.”

Finally, the Commentary to the HPCR Manual states—without recorded dissent among the group of experts—that “whereas a particular course of action may be considered non-feasible due to military considerations (such as excessive risks to aircraft and their crews), some risks have to be accepted in light of humanitarian considerations.” Evidently, “excessive risks” to attackers are risks that are excessive in relation to the relevant humanitarian considerations. If a course of action would greatly increase risk to attackers and only slightly reduce risk to civilians then the attackers do not have to accept such excessive risks. Conversely, if a course of action would slightly increase risk to attackers and greatly reduce risk to civilians then the attackers have to accept such reasonable risks.

On this balanced approach, the precautions rule does not require soldiers to take suicidal risks, or to doom an otherwise lawful mission, in order to avoid any risk of harming civilians. However, the precautions rule

---

64. Id. at 177.
67. Schmitt, supra note 57, at 462. For my views, see Haque, supra note 12, at 106–10.
68. Dinstein, supra note 5, at 141.
69. COMMENTARY ON THE HPCR MANUAL, supra note 10, at 39.
may require attackers to accept some additional risk in order to reduce the risks that their actions pose to civilians. Here, as elsewhere, there will be hard cases in which reasonable commanders must exercise their professional judgment—with which reasonable observers may in turn disagree. However, as elsewhere, there will also be clear cases in which any reasonable commander would accept some risk to attacking forces or to mission success in order to entirely avoid or greatly reduce the possibility of needlessly killing civilians.

B. The Manual

The Manual recognizes that “[p]arties to a conflict must take feasible precautions to reduce the risk of harm to the civilian population and other protected persons and objects.”70 The Manual also accepts that feasible precautions are those precautions that are “practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations.”71 However, the Manual asserts that

if a commander determines that taking a precaution would result in operational risk (i.e., a risk of failing to accomplish the mission) or an increased risk of harm to their own forces, then the precaution would not be feasible and would not be required.72

In other words, if taking a precaution would even slightly increase risk to attacking forces or to mission success then that precaution is infeasible per se, even if taking that precaution would entirely avoid or greatly reduce risk to civilians. Returning to the case with which this section began, according to the Manual, it would be perfectly lawful to strike the house with a missile, certainly killing five children, rather than raid the house, killing no children, while placing attacking forces at only slightly greater risk. Put another way, if the proportionality rule does not prohibit a missile strike then the precautions rule does not require a raid.

---

70. DoD Manual, supra note 1, ¶ 5.3.3 (“Feasible precautions to reduce the risk of harm to civilians and civilian objects must be taken when planning and conducting attacks.”). See also id. ¶ 5.11 (“Combatants must take feasible precautions in conducting attacks to reduce the risk of harm to civilians and other protected persons and objects.”).
71. Id. ¶ 5.3.3.2.
72. Id.
It seems that, according to the Manual, "feasible" precautions are not all precautions that are practicable or practically possible but instead only precautions that are free of risk to the attacking force. Far from taking into account both humanitarian and military considerations, the Manual seems to disregard or exclude the former when they conflict with the latter—as they almost always do.

To see that the DoD's view is dangerously unbalanced, imagine if a human rights group asserted the following:

If a commander determines that failing to take a precaution would result in an increased risk of harm to civilians, then the precaution is feasible and is required.

Such a view would be dismissed immediately, since it gives humanitarian considerations absolute priority over military considerations while the precautions rule requires taking into account both humanitarian and military considerations. Yet the DoD's position goes just as far, except in the opposite direction. The DoD's position gives military considerations absolute priority over humanitarian considerations in determining an attacker's precautionary obligations. Neither view strikes a reasonable balance between the guiding concerns of the law of war.

The DoD appears to differ on this point with the U.S. Joint Chiefs of Staff, who in 2013 took the position that "circumstances permit" effective advance warning of an attack when "any degradation in attack effectiveness is outweighed by the reduction in collateral damage [e.g.,] because advanced warning allowed the adversary to get civilians out of the target area."73 On this balanced view, attackers must weigh the military reasons to attack without warning against the humanitarian reasons to give advance warning. If the latter outweigh the former then advance warning must be given; if not, then not.

Indeed, U.S. targeting practice routinely accepts some risk to attacking forces in order to avoid harming civilians. For example, in a 1991 letter to the UN Secretary General regarding its conduct of hostilities with Iraq, the United States stressed that "allied aircraft involved in these attacks are taking every precaution to avoid civilian casualties. These pilots are in fact placing themselves in greater danger in order to minimize collateral damage.

and civilian casualties.\textsuperscript{74} In a subsequent report to Congress, the U.S. Department of Defense stated that: “U.S. forces have taken reasonable measures to minimize collateral injury to civilians and damage to civilian objects while conducting their military operations, often at increased risk to U.S. personnel.”\textsuperscript{75} U.S. forces seem to recognize that legitimate warfighting requires that they accept reasonable risks in order to avoid harming civilians. As former Air Force pilot Chris Stewart writes: “I... never met a pilot or crewmember in the U.S. Air Force who was not willing to take at least some risk to avoid being the one to drop his ordnance atop women, children, hospitals or a passenger train. That is the way Americans conduct war.”\textsuperscript{76} According to Charles Dunlap, the “disposition to so readily balance potential military losses against expected enemy civilian fatalities is rooted deep in the American psyche.”\textsuperscript{77}

In support of its position, the Manual cites no U.S. practice of foregoing precautions that would greatly reduce risk to civilians while only slightly increasing risk to attacking forces, let alone accompanying\textit{ opinio juris} that such conduct is lawful. Instead, the Manual cites the 1991 telegram to the ICRC discussed earlier:

“We feasible precautions” are reasonable precautions, consistent with mission accomplishment and allowable risk to attacking forces. While collateral damage to civilian objects should be minimized, consistent with the above, collateral damage to civilian objects should not be given the same level of concern as incidental injury to civilians. Measures to minimize collateral damage to civilian objects should not include steps that will place U.S. and allied lives at greater or unnecessary risk.\textsuperscript{78}


\textsuperscript{77} Dunlap, supra note 76, at 100.

\textsuperscript{78} DO\textsuperscript{D} MANUAL, supra note 1, ¶ 5.3.3.2 n.39 (quoting U.S. Comments, supra note 37, at 2057, 2063).
Nowhere does the telegram state that any operational risk or risk to attacking forces renders a precaution unreasonable, infeasible, or otherwise optional. On the contrary, a precaution that only slightly increases operational risk may be “consistent with mission accomplishment.” Similarly, a precaution that only slightly increases risk to attacking forces may be “allowable.” The Manual contains no such qualifications.

Importantly, the telegram states that measures to minimize collateral damage to civilian objects should not include steps that will place U.S. and allied lives at greater risk. In contrast, the telegram does not say that measures to minimize incidental injury to civilians should not include steps that will place U.S. and allied lives at greater risk. On the contrary, the telegram states that “collateral damage to civilian objects should not be given the same level of concern as incidental injury to civilians.”79 Presumably, this sentence means that injury to civilians should be given a higher level of concern than damage to civilian objects. It seems to follow that measures to minimize incidental injury to civilians may include steps that will place attackers at greater risk, at least when the greater risk to attackers is clearly outweighed by the reduced risk to civilians. If anything, the telegram undercuts rather than supports the position of the Manual.

According to the Manual, the precautions rule never requires attackers to accept “an increased risk of harm to their own forces.”80 In contrast, according to the telegram, the precautions rule requires attackers to accept “allowable risk to attacking forces.”81 Some readers may hope that the citation to the telegram is intended to qualify the seemingly unqualified language of the text. However, according to the Manual,

it was desirable that this manual’s main text convey as much information as possible without the reader needing to read the footnotes. For example, it was desirable to avoid the possibility that a reader might misunderstand a legal rule addressed in the main text because a notable exception to that rule was addressed only in a footnote accompanying the text.82

79. Id. (emphasis added).
80. DOD MANUAL, supra note 1, ¶ 5.3.3.2.
81. Id. ¶ 5.3.3.2 n.39 (quoting U.S. Comments, supra note 37, at 2057, 2063).
82. Id. ¶ 1.2.1
This passage suggests that sources quoted in footnotes are not intended to significantly modify propositions put forward in the text.83

The *Manual* itself offers no direct argument for its interpretation of the precautionary principle, but we might cobble one together from pieces of an earlier section. Consider the following claims made by the *Manual*:

*Military necessity* may be defined as the principle that justifies the use of all measures needed to defeat the enemy as quickly and efficiently as possible that are not prohibited by the law of war.94

Certain law of war rules may direct that persons comply with an obligation, but only to the extent feasible or consistent with *military necessity*. Examples of rules incorporating the concept of *feasibility* or *necessity* include the following:

- Certain affirmative duties to take *feasible* precautions to reduce the risk of harm to the civilian population and other protected persons and objects.95

These passages suggest that, according to the *Manual*, a feasible precaution is one that is consistent with military necessity, that is, with defeating the enemy as quickly and efficiently as possible. It would follow that any precaution that might make defeating the enemy more difficult is *ipso facto* infeasible and therefore not legally required.

This approach is clearly mistaken. While military necessity reflects only military considerations, the feasibility of a precaution takes into account both humanitarian and military considerations. It is therefore incorrect to equate feasibility with military necessity alone. As the *Manual* elsewhere states, “[t]he extent to which military necessity justifies [incidental] harms [to civilians] is addressed by the principle of proportionality.”86 As we shall see, the principle of proportionality, not the principle of military necessity, determines the scope of our precautionary obligations.

83. As an aside, according to the *Manual*, the absence of an introductory signal indicates that a source directly states the proposition for which it is cited while sources that support a proposition are introduced by “see” and sources that elaborate upon a proposition are introduced by “see also.” *Id.* ¶ 1.2.4. This is some evidence (of course not alone dispositive) that the authors of the *Manual* believed that the telegram directly states the proposition contained in the text rather than merely supporting it or elaborating upon it.
84. DOd Manual, supra note 1, ¶ 2.2.
85. Id. ¶ 2.2.2.2.
86. Id. ¶ 2.2.1.
C. Logic

Interestingly, the Manual distinguishes between the proportionality principle and the proportionality rule. The proportionality principle "generally weighs the justification for acting against the expected harms to determine whether the latter are disproportionate in comparison to the former." In contrast, the proportionality rule specifically "obliges persons to refrain from attacking where the expected harm incidental to such attacks would be excessive in relation to the military advantage anticipated to be gained." According to the Manual, [t]he principle of proportionality is reflected in many areas in the law of war.

Proportionality most often refers to the jus in bello standard applicable to persons conducting attacks. Proportionality considerations, however, may also be understood to apply to the party subject to attack, which must take feasible precautions to reduce the risk of incidental harm.

Of course, persons conducting attacks also must take feasible precautions to reduce the risk of incidental harm. It seems to follow that proportionality considerations should inform the precautionary obligations of both attackers and defenders.

What would it mean for attackers or defenders to apply proportionality considerations to their precautionary obligations? It seems logical that they should weigh the justification for acting without taking a precaution against the expected harms of not taking that precaution to determine whether the latter are disproportionate in comparison to the former. If choosing different weapons or tactics would place civilians at much less risk and would place soldiers at only slightly greater risk, then they must be chosen. Conversely, if choosing different weapons or tactics would place civilians at only slightly less risk and would place soldiers at much greater risk, then they need not be chosen. When the risks on each side are more closely balanced, military commanders must exercise reasonable judgment based on the information available to them at the time.

87. Id. ¶ 2.4.1.2.
88. Id.
89. Id. ¶ 2.4.2.
On this approach, the precautions rule and the proportionality rule work together to balance humanitarian and military considerations across the targeting process. The proportionality rule weighs the overall military considerations in favor of an attack against the overall humanitarian considerations against an attack. In contrast, the precautions rule balances the marginal military considerations in favor of attacking using particular means and methods against the marginal humanitarian considerations in favor of attacking using alternative means and methods.90

Indeed, it would be illogical for the law of war to determine whether attacks may be carried out based on humanitarian considerations but not to regulate how attacks may be carried out based on humanitarian considerations. Put another way, the proportionality rule can prohibit the pursuit of a military advantage while the precautions rule can only regulate the pursuit of a military advantage. It makes no sense for humanitarian considerations to inform the more restrictive rule but not the less restrictive rule.

To see the illogic of the Manual even more clearly, consider that often the military advantage anticipated from an attack lies precisely in its contribution to the success of future missions or to the future safety of the attacking force. Nevertheless, if the expected harm to civilians is excessive in relation to the anticipated reduction in future operational and personal risk, then the attack is flatly prohibited by the proportionality rule. Yet, according to the Manual, humanitarian considerations that can outweigh operational and personal risk under the proportionality rule count for nothing under the precautions rule. We might be forced to accept such an illogical result by strong evidence or argument that the result is compelled by treaty or custom. As we have seen, the Manual provides no such evidence.

IV. PROPORTIONALITY AND HUMAN SHIELDS

An ordinary combatant takes refuge in an apartment building, for the specific purpose of using the presence of the residents to dissuade your forces from attacking him. Most of the residents are unaware of his presence. Others are too young, old, sick or infirm to leave. Your armed forces have no troops on the ground and no way to warn those residents who can leave

90. See Seth Lazar, Neccessity in Self-Defense and War, 40 PHILOSOPHY AND PUBLIC AFFAIRS 3, 43 (2012) ("When comparing options that involve different degrees of risk to civilians and to friendly combatants, we must ask whether the additional marginal risk imposed on civilians is justified by the marginal reduction in risk to combatants.").
to do so. The most discriminate weapons and tactics available to you will destroy half of the building, killing scores of residents.

As a legal officer, what would you advise? As a commander, what would you order? As an operator, what order would you obey?

A. The Law

Article 51 of Protocol I declares that

The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations. To give effect to this protection, the following rules, which are additional to other applicable rules of international law, shall be observed in all circumstances.91

The same article later states the proportionality rule that protects civilians from attacks "which may be expected to cause incidental loss of civilian life . . . which would be excessive in relation to the concrete and direct military advantage anticipated."92 One sentence later, the very same article categorically prohibits using civilians as human shields, either by moving civilians near military objectives (active shielding) or by moving military objectives near civilians (passive shielding) for the purpose of shielding those objectives from attack.93 Finally, the next sentence states that "any violation of these prohibitions shall not release the [other] Parties to the conflict from their legal obligations with respect to the civilian population."94

The import of Protocol I is unmistakable. The proportionality rule shall be observed in all circumstances. In particular, one party's unlawful use of civilians as human shields shall not release other parties from their legal obligation not to knowingly inflict incidental harm on those civilians that would be excessive in relation to the anticipated advantage.95 Returning to the scenar-

91. Protocol I, supra note 18, art. 51(1).
92. Id. art. 51(5)(b). See also id. art. 57(2)(a)(ii).
93. Id. art. 51(7). On some views, civilians who freely serve as voluntary human shields directly participate in hostilities and thereby forfeit their civilian immunity. One counter-intuitive implication of this view is that such civilians lose their legal protection against being used as human shields and hence it is not unlawful to use them as such.
94. Id. art. 51(8).
95. See, e.g., Australian Department of Defence, ADDP 3.14, Targeting ¶ 3.12 (2009) ("Breaches of obligations by a party. A party is still required to apply the protections in Additional Protocol I (including the precautions required by Article 57), notwithstanding that the enemy attempts to shield military objectives from attacks or to shield, favour or
io with which this part began, under Protocol I it would be unlawful to attack the apartment building, killing scores of residents, in order to kill one ordinary combatant. This approach seems normatively sound. The residents should not lose their rights through no fault of their own, and it would be wrong to punish them for the crimes that the combatant commits against them.

Importantly, most international lawyers distinguish between voluntary shields and involuntary shields. Voluntary shields are civilians who freely choose to remain in or near military objectives, specifically intending to thereby prevent or dissuade attacks on those objectives.\(^6\) Involuntary shields are civilians who are used by defending forces to prevent or dissuade attacks on nearby military objectives against their will, without their knowledge, or without their consent.\(^7\) Although the legal status of voluntary shields remains controversial, many experts argue that voluntary shields directly participate in hostilities and thereby lose their protection under the proportionality rule.\(^8\) In contrast, most international lawyers agree that involuntary shields retain their protection under the proportionality rule.\(^9\) This part will focus on the status of involuntary shields, for reasons that will soon become clear.

On this balanced view, attacking forces must compare the collateral harm that they expect to inflict on involuntary shields with the military advantage that they expect to obtain from their attack. If the anticipated advantage is great and the expected harm is small then the attack is lawful. Conversely, if the expected harm is great and the anticipated advantage is small then the attack is unlawful. On this balanced view, the presence of involuntary shields does not automatically preclude an attack. Nor, however, does the fact that civilians are involuntary shields—rather than unwitting passersby—automatically permit an attack. Here, as elsewhere, the law-

---

impede military operations, by the presence or movement of civilians."\(^{6}\)). Note that Article 57(2)(a)(iii) of Protocol I repeats the proportionality rule.

\(^6\) See, e.g., COMMENTARY ON THE HPCR MANUAL, supra note 10, at 144.

\(^7\) Id.

\(^8\) Id. But see INTERPRETIVE GUIDANCE, supra note 2, at 41–64; IAN HENDERSON, THE CONTEMPORARY LAW OF TARGETING 217–18 (2009); ADIL AHMAD HAQUE, LAW AND MORALITY AT WAR ch. 9 (forthcoming 2016).

\(^9\) Id. The UK Manual suggests that, under Protocol I, a defender’s use of human shields is “a factor to be taken into account in favour of the attackers in considering the legality of attacks.” UK MANUAL, supra note 59, ¶ 2.7.2. I examine and reject this position elsewhere. See HAQUE, supra note 98, ch. 9. For now it is sufficient to note that the UK Manual accepts that harm to human shields can render an attack disproportionate.
fulness of an attack depends on the balance of military considerations in favor of attack and humanitarian considerations against attack.

So much for the 174 parties to Protocol I. What about the 19 non-signatories to Protocol I, including the United States, Iran, Israel, and Sri Lanka? Is it possible that, under customary law, the proportionality rule need not be observed in all circumstances? Is it possible that, under customary law, one party’s use of civilians as involuntary shields releases opposing parties from their legal obligation not to inflict otherwise excessive harm on those civilians?

Such a view defies the general principle of customary international law that “[t]he obligation to respect and ensure respect for international humanitarian law does not depend on reciprocity.” Under customary law, each party’s legal obligations with respect to the civilian population apply categorically, unconditionally and independently of the conduct of the opposing party. After all, these legal obligations are not owed to the opposing party but to the civilian population. These legal obligations rest not on considerations of fairness or reciprocity but on considerations of humanity.

To see the same point from a different angle, consider that the legal obligations of combatants correspond to and are grounded in the legal rights of civilians. Under international law, “individual civilians shall enjoy general protection against dangers arising from military operations . . . unless and for such time as they take a direct part in hostilities.” More broadly, civilians can only lose their legal rights through their own conduct. Conversely, civilians cannot lose their legal rights due to the illegal conduct of others. As Michael Schmitt puts it, “A Party to the conflict [that] is placing the civilians at risk in order to enhance its military position . . . should not be permitted to deprive civilians of the protections to which they are entitled under the LOAC.”

Put another way, the “in all circumstances” provision and the “shall not release” provision of Protocol I are not substantive norms that may be rejected while the principles of distinction, precautions, and proportionality are accepted. Instead, the two provisions are declaratory norms, and what they declare is the unconditional application of the principles of distinction,

100. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, supra note 6, at 498.
101. Protocol I, supra note 18, arts. 51(1), 51(3). See also CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, supra note 6, at 19.
precautions, and proportionality. One cannot endorse the principles of distinction, precautions, and proportionality only on the condition that the opposing party fulfills its legal obligations. On the contrary, it is constitutive of the principles of distinction, precautions, and proportionality that they apply unconditionally.

With these general considerations in mind, let us turn to specifics. According to the ICRC,

State practice indicates that an attacker is not prevented from attacking military objectives if the defender fails to take appropriate precautions or deliberately uses civilians to shield military operations. The attacker remains bound in all circumstances, however, to take appropriate precautions in attack and must respect the principle of proportionality even though the defender violates international humanitarian law.103

Put more precisely, an attacker is not automatically prevented from attacking military objectives if the defender uses civilians to shield military operations. In contrast, if the expected harm to involuntary shields would be excessive in relation to the anticipated military advantage then the attacker must respect the principle of proportionality even though the defender violates international humanitarian law.

For example, Israel is not a party to Protocol I and regularly faces adversaries that use civilians as human shields. Arguably, Israel is even a “specially affected State” with “a distinctive history of participation in the relevant matter, . . . that ha[s] had a wealth of experience, or that ha[s] otherwise had significant opportunities to develop a carefully considered military doctrine” and whose practice is therefore particularly significant.104 Famously, the Israeli Supreme Court holds that when “civilians are forced to serve as “human shields” . . . the rule is that the harm to the innocent civilians must fulfill, inter alia, the requirements of the principle of proportionality.”105 The official position of the Israeli Defense Forces remains that, “[w]ith respect to involuntary shields, Israel adopts the majority view that involuntary shields retain all civilian protection. An attacker . . . must consider their presence when making proportionality calculations.”106

103. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, supra note 6, at 71.
104. DOD MANUAL, supra note 1, ¶ 1.8.2.3.
106. Schmitt & Merriam, supra note 102, at 117.
The ICRC found no contrary practice among States that are not party to Protocol I. In addition, no State party to Protocol I has stated that harm to involuntary shields may be excluded from the proportionality rule in non-international armed conflicts to which Protocol I does not apply. Since the use of involuntary shields is particularly common in non-international armed conflicts, the absence of contrary practice on this point is particularly telling.

Finally, according to Michael Schmitt, the view that “treats involuntary shields as civilians entitled to the full benefits of their international humanitarian law protections[,]” “seems to dominate among international humanitarian law experts.”\(^{107}\) Schmitt elsewhere describes the opposing view, that harm to involuntary shields may be entirely disregarded in determining the proportionality of an attack, as “an extreme view that has, fortunately, gained little traction.”\(^{108}\)

**B. The Manual**

From 2002 to 2013, the U.S. Joint Chiefs of Staff consistently took the position that

Joint force targeting . . . is driven by the principle of proportionality, so that otherwise lawful targets involuntarily shielded with protected civilians may be attacked . . . provided that the collateral damage is not excessive compared to the concrete and direct military advantage anticipated by the attack.\(^{109}\)

While U.S. forces were engaged in over a decade of irregular warfare against armed groups that used civilians as involuntary shields, the Joint


\(^{109}\) Joint Publication 3-60 (2013), *supra* note 73, at A-2. *See also* Chairman, Joint Chiefs of Staff, Joint Publication 3-60, *Joint Targeting*, A-2–A-3 (2002) (“Civilians may not be used as human shields in an attempt to protect, conceal, or render military objects immune from military operations . . . Joint force responsibilities during such situations are driven by the principle of proportionality as mentioned above.”).
Chiefs consistently maintained that such civilians “have not lost their protected status” and remain protected by the proportionality rule. 110

Unfortunately, the Manual departs from the balanced view of the U.S. Joint Chiefs of Staff, the IDF, the ICRC, and the majority of law of war experts. The Manual takes the following position:

Harm to the following categories of persons and objects would be understood not to prohibit attacks under the proportionality rule: (1) military objectives [that is, enemy combatants, civilians taking a direct part in hostilities, and military equipment]; (2) certain categories of individuals who may be employed in or on military objectives; and (3) human shields. 111

Strikingly, the Manual draws no distinction between civilians who freely choose to serve as voluntary human shields and civilians forced to serve as involuntary human shields. According to the Manual, neither harm to voluntary shields nor harm to involuntary shields will prohibit attacks under the proportionality rule.

Recall the scenario with which we began. According to the Manual, the proportionality rule would not prohibit an attack on the apartment building, despite the fact that the expected deaths of scores of residents would be clearly excessive in relation to the concrete and direct military advantage anticipated from killing one ordinary combatant. Since the combatant intends to use the residents to shield himself from attack, harm to the residents is effectively excluded from the proportionality rule. According to the Manual, as far as proportionality is concerned, the residents may as well not exist.

The Manual’s position generates other illogical results. Consider the following scenario:

Military targets A and B are weapons caches containing the same number of rifles. Ten civilians are unwittingly passing by target A. Twenty civilians are forced to serve as involuntary human shields for target B.

If the military advantage anticipated by destroying the weapons in each cache is fairly small then it might be disproportionate to strike target A,

---

110. Chairman, Joint Chiefs of Staff, Joint Publication 3-60, Joint Targeting, E-2–E-3 (2007) (“[A] defender may not use civilians as human shields . . . . In these cases, the civilians have not lost their protected status and joint force responsibilities during such situations are driven by the principle of proportionality.”).

111. DoD Manual, supra note 1, ¶ 5.12.3.
killing ten civilians. However, according to the Manual, it is necessarily proportionate to strike target B, killing twenty civilians, because those civilians are being used as involuntary human shields. This result seems illogical. If a military advantage cannot justify killing ten civilians who have done nothing to forfeit their legal rights then an equivalent military advantage cannot justify killing twenty civilians who also have done nothing to forfeit their legal rights.

To see a subtler problem with the Manual’s position, compare the following scenarios:

1. An ordinary combatant runs through a crowded market because that is the fastest route to his destination. Attacking him will kill many nearby civilians.

On any plausible view, the proportionality rule would prohibit attacking the combatant in scenario 1, because the expected collateral harm is great and the anticipated military advantage is small. Now consider the following variation:

2. The same combatant runs through the same market because he hopes that he will not be attacked with so many civilians nearby. Attacking him will kill the same number of nearby civilians.

According to the Manual, the proportionality rule would permit attacking the combatant in scenario 2 because he is using the nearby civilians as human shields. Yet it seems illogical that the lawfulness of killing the nearby civilians should turn on the combatant’s mental state—his purpose or motive for co-locating with civilians—rather than on the expected harm to the civilians and the anticipated military advantage of killing the combatant.

A legal position that generates such illogical results should be rejected absent overwhelming evidence in its favor. Remarkably, the Manual offers none. The Manual cites no State practice or opinio juris directly supporting its claim that harm to human shields cannot render an attack disproportionate. Since the proportionality rule states a general prohibition, the Manual bears the burden of establishing a specific exception or exemption to that general prohibition.

Interestingly, the Manual does not suggest that human shields directly participate in hostilities or are otherwise military objectives. Nor does the Manual suggest that, like civilians who work in or on military objectives, human shields “are deemed to have assumed the risk of incidental harm
from military operations" and therefore lose their protection under the proportionality rule.112 Finally, the Manual does not suggest that there is some additional military advantage to attacking military objectives protected by human shields that offsets the expected loss of civilian life.113

Instead, the Manual states the following:

Use of human shields violates the rule that civilians may not be used to shield, favor, or impede military operations. The party that employs human shields in an attempt to shield military objectives from attack assumes responsibility for their injury, provided that the attacker takes feasible precautions in conducting its attack.

If the proportionality rule were interpreted to permit the use of human shields to prohibit attacks, such an interpretation would perversely encourage the use of human shields and allow violations by the defending force to increase the legal obligations on the attacking force.114

It is not clear whether these statements are intended de lege lata or de lege ferenda. I will consider each of these statements in the following sections, both as a matter of law and as a matter of logic.

Interestingly, in a 1990 law review article, W. Hays Parks writes that

While an attacker facing a target shielded from attack by civilians is not relieved from his duty to exercise reasonable precautions to minimize the loss of civilian life, neither is he obligated to assume any additional responsibility as a result of the illegal acts of the defender. Were an attacker to do so, his erroneous assumption of additional responsibility with regard to protecting the civilians shielding a lawful target would serve as an

112. Id. ¶ 5.12.3.2. In fact, harm to munitions workers can render an attack unlawful under the proportionality rule. See, e.g., UK Manual, supra note 59, ¶ 2.5.2, at 24 (stating that "munitions factories are legitimate military targets and civilians working there, though not themselves legitimate targets, are at risk if those targets are attacked. Such incidental damage is controlled by the principle of proportionality"); Commentary on the HPCR Manual, supra note 10, at 93–94 ("The majority of the Group of Experts felt that the principle of proportionality applies to such civilians as in all other cases.").

113. As I argue elsewhere, the advantage anticipated from preventing one's adversary from preventing an attack through the use of human shields is just the advantage anticipated from the attack itself. See Haque, supra note 98, ch. 9.

114. DoD Manual, supra note 1, ¶ 5.12.3.3.
incentive for a defender to continue to violate the law of war by exposing other innocent civilians to similar risk. 115

Parks later chaired the DoD working group that prepared the Manual, from 1996 until 2010. 116 Although the Manual does not cite Parks’ article in its discussion of human shields, the similarities between the two suggests that Parks’ views may have influenced its formation. We should therefore consider any additional evidence or arguments contained in Parks’ article.

First, we should consider whether the Manual’s basic position—that no amount of expected incidental harm to human shields can render an attack unlawfully disproportionate—has any basis in U.S. practice. We have already seen that the U.S. Joint Chiefs have consistently maintained that involuntary shields retain their protection under the proportionality rule. What of the various branches of the U.S. Armed Forces?

The Commander’s Handbook on the Law of Naval Operations rewards close reading. The applicable passage says that

Deliberate use of civilians to shield military objectives from enemy attack is prohibited. Although the principle of proportionality underlying the concept of collateral damage continues to apply in such cases, the presence of civilians within or adjacent to a legitimate military objective does not preclude attack of it. Such military objectives may be lawfully targeted and destroyed as needed for mission accomplishment. In such cases, responsibility for the injury and/or death of such civilians, if any, falls on the belligerent so employing them. 117

Since the principle of proportionality “continues to apply” to involuntary shields, the claim that their presence “does not preclude attack” on shielded objectives can only mean that the presence of involuntary shields does not automatically or necessarily preclude attack on shielded objectives. Instead, such attacks are precluded if and only if they would be disproportionate. Similarly, the claim that “responsibility for the injury and/or death of such

---

citizens, if any, falls on the belligerent so employing them” can only mean that if the principle of proportionality is satisfied then responsibility falls on the defender but not the attacker. Conversely, if the principle of proportionality is violated then responsibility falls on both the defender that unlawfully uses human shields and the attacker that unlawfully kills human shields.

To see this point more clearly, contrast the previous passage with the immediately following passages:

The presence of civilian workers, such as technical representatives aboard a warship or employees in a munitions factory, in or on a military objective, does not alter the status of the military objective. These civilians may be excluded from the proportionality analysis.

Civilians who voluntarily place themselves in or on a military objective as “human shields” in order to deter a lawful attack do not alter the status of the military objective. While the law of armed conflict is not fully developed in such cases, such persons may also be considered to be taking a direct part in hostilities or contributing directly to the enemy’s warring/war-sustaining capability, and may be excluded from the proportionality analysis.118

The Handbook explicitly states that civilian workers and voluntary shields may be excluded from the proportionality analysis. In sharp contrast, the Handbook does not say that involuntary shields may be excluded from the proportionality analysis. This sharp contrast between adjacent provisions implies that involuntary shields may not be excluded from the proportionality analysis.

In 2011, the U.S. Air Force targeting doctrine endorsed the proportionality rule and nowhere excluded harm to involuntary shields from its application or interpretation.119 Instead, the Air Force stated that

citizens may not be used as “human shields” to protect military targets from attack. The fact that they may be used to do so does not necessarily prevent the military object from being attacked. As directed or time permitting, targets surrounded by human shields will probably need to be re-

118. Id. at 8-4 (emphasis added).
viewed by higher authority for policy and legal considerations based on the specific facts.\textsuperscript{120}

Indeed, the use of involuntary shields does not necessarily prevent military objects from being lawfully attacked. Nevertheless, the use of involuntary shields may render an attack unlawful under the proportionality rule.

In 2014, the U.S. Air Force Judge Advocate General’s School explained that

Where civilians are present on the battlefield or in proximity to legitimate military objectives, or are being used to shield legitimate targets from an attack that otherwise would be lawful, they are at risk of injury incidental to the lawful conduct of military operations. A law of armed conflict violation occurs where the civilian population is attacked intentionally, where collateral civilian casualties become excessive in relation to military necessity; and/or where a defender or attacker employs civilians as voluntary or involuntary human shields. Each constitutes a violation of the principle of distinction.\textsuperscript{121}

Indeed, involuntary shields are at risk of injury incidental to the lawful conduct of military operations. In contrast, an attack that otherwise would be lawful is a law of armed conflict violation where collateral civilian casualties become excessive in relation to military necessity. Tellingly, the Air Force JAG School draws no distinction between civilians present on the battlefield or in proximity to legitimate military objectives and civilians being used as involuntary shields. The proportionality rule protects them both equally.

Elsewhere, the Air Force JAG School notes that a “nation that uses its civilian population to shield its own military forces violates the law of war at the peril of the civilians behind whom it hides.”\textsuperscript{122} Importantly, this statement appears in a discussion of the principle of distinction, expressing the obligation of defenders to distinguish themselves from their civilian population. When the authors discuss the principle of proportionality, a mere five sentences later, involuntary shields are not even mentioned. The authors later clarify that “the use of human shields does not necessarily

\textsuperscript{120} Id. at 90.


\textsuperscript{122} Id. at 271.
prevent the military object from being attacked.\textsuperscript{123} In contrast, as we have seen, an attack that inflicts excessive harm on civilians not taking direct part in hostilities—including involuntary shields—is a law of armed conflict violation. It therefore seems that the Manual departs from consistent U.S. practice.

In his 1990 article, Parks took the view that

Excluded in determination of collateral civilian casualties are: ... civilians injured or killed as a result of the enemy placing them around a lawful target in an effort to shield it from attack.\textsuperscript{124}

Naturally, Parks' article could not anticipate U.S. practice, Israeli practice, or other State practice in the twenty-six years since its publication. Most of the State practice cited in the article pre-dates the adoption of Protocol I. Since Protocol I crystallized the proportionality rule—and affirmed that the rule rests on humanity irrespective of reciprocity—State practice prior to 1977 is inherently unreliable evidence that customary international law exempts human shields from protection under the proportionality rule.

In any event, Parks' article does not identify a single example of a State applying the proportionality rule while excluding human shields from its protection. Of course, States have carried out attacks on military objectives despite the presence of human shields. It hardly follows that these States excluded expected harm to human shields from their proportionality analysis. They may have determined that the expected harm to human shields was outweighed by the anticipated military advantage. Alternatively, these States may not have conducted a serious proportionality analysis at all. As leading U.S. lawyers elsewhere explain,

Although the same action may serve as evidence both of State practice and \textit{opinio juris}, the United States does not agree that \textit{opinio juris} simply can be inferred from practice.

\ldots

A more rigorous approach to establishing \textit{opinio juris} is required. It is critical to establish by positive evidence, \ldots that States consider themselves

\textsuperscript{123} Id. at 273.
\textsuperscript{124} Parks, \textit{supra} note 115, at 174.
legally obligated [or permitted] to follow the courses of action reflected in [purported] rules.\textsuperscript{125}

Such positive evidence of \textit{opinio juris} is essential to distinguish State practice that reflects or generates customary law from State practice that misapplies or violates customary law. \textit{Opinio} without \textit{usus} is sometimes empty, but \textit{usus} without \textit{opinio} is always blind.

Remarkably, in 225 pages, which include 663 footnotes, Parks identifies only one source that explicitly states that the proportionality rule excludes harm to involuntary shields: an unpublished 1983 document entitled “Proportionality in a Nutshell” written by Parks himself.\textsuperscript{126} Simply put, Parks’ article identifies no State practice or \textit{opinio juris} supporting the categorical exclusion of harm to involuntary shields from the proportionality rule.\textsuperscript{127}

Importantly, Parks writes that “The classic example of a disproportionate action is the destruction of a village of 500, including its population, to destroy a single enemy sniper or machine gun position.”\textsuperscript{128} Yet, if the sniper or gunner positions himself in the village for the specific purpose of using the proximity of civilians to prevent or dissuade an attack on his position then he uses those civilians as passive, involuntary human shields. As we have seen, according to Parks, expected harm to involuntary shields should be excluded from the application of the proportionality rule. It follows that Parks’ “classic example of a disproportionate action” is, according to Parks’ own view, perfectly proportionate after all. This implication seems like a \textit{reductio ad absurdum} of the view from which it derives.


\textsuperscript{126} Parks, supra note 115, at 174.

\textsuperscript{127} Unfortunately, Parks’ article seems to be cited more often than it is critically examined. For example, Yoram Dinstein writes that, under customary international law, “should civilian casualties ensue from an illegal attempt to shield combatants or a military objective, the ultimate responsibility lies with the Belligerent Party placing civilians at risk.” \textit{Dinstein, supra 5}, at 155. In support of this claim, Dinstein cites only two sources: Parks’ article and a student comment that in turn cites only Parks’ article.

\textsuperscript{128} Parks, supra note 115, at 168.
C. Responsibility

As we have seen, the Manual asserts that:

The party that employs human shields in an attempt to shield military objectives from attack assumes responsibility for their injury, provided that the attacker takes feasible precautions in conducting its attack. 129

It seems that, according to the Manual, a defender’s “responsibility” for expected harm to human shields relieves an attacker of its “responsibility” for expected harm to human shields, provided that the attacker takes feasible precautions in conducting its attack. On this view, attackers may not inflict unnecessary harm on human shields but attackers may inflict disproportionate harm on human shields or, more precisely, expected harm that would ordinarily be considered excessive in relation to the anticipated military advantage. As we shall see, this argument has no basis in law or logic.

1. Law

In support of its argument, the DoD cites two U.S. sources: an instructor training document from 1975 and the 1991 telegram to the ICRC discussed earlier. 130 Since the training document predates Protocol I and is clearly not an official expression of opinio juris, I will discuss it no further. The telegram to the ICRC is worth reading closely. Recall that the telegram is a point-by-point response to an ICRC memorandum. Paragraph 4B(1) of the ICRC memorandum states that

A distinction must be made in all circumstances between combatants and military objectives on the one hand, and civilians and civilian objects on the other. It is forbidden to attack civilian persons or objects or to launch indiscriminate attacks. 131

In direct response to this paragraph, the telegram says that

In no case may a combatant force utilize individual civilians or the civilian population to shield a military objective from attack. A nation that utilizes

129. DOD MANUAL, supra note 1, ¶ 5.12.3.3.
130. Id. ¶ 5.12.3.3 n.315.
131. U.S. Comments, supra note 37, at 2057, 2059 (emphasis added).
civilians to shield a target from attack assumes responsibility for their injury, so long as an attacker exercises reasonable precaution in executing its operations.\textsuperscript{132}

Read alongside the passage of the ICRC memorandum to which it directly responds, this passage of the telegram says that harm to human shields will not render an attack \textit{indiscriminate} so long as an attacker exercises reasonable precaution in executing its operations. So understood, this passage of the telegram seems sound. Presumably, reasonable precaution in executing operations includes directing attacks at specific military objectives, using means and methods of combat that can be so directed and the effects of which can be limited as required by international humanitarian law.

Crucially, the \textit{Manual} cites the quoted passage of the telegram in support of its position that harm to human shields will not render an attack \textit{disproportionate}.\textsuperscript{133} Yet, as we have seen, neither this passage of the telegram nor the passage of the memorandum to which it directly responds says anything about the proportionality rule. Instead, the ICRC invokes the proportionality rule for the first time in the next paragraph of its memo, 4B(2):

\begin{quote}
All feasible precautions must be taken to avoid loss of civilian life or damage to civilian objects, and attacks that would cause incidental loss of life or damage which would be excessive in relation to the direct military advantage anticipated are prohibited.\textsuperscript{134}
\end{quote}

In direct response to \textit{this} paragraph, the telegram makes four comments on the nature and application of the proportionality rule.\textsuperscript{135} Revealingly, nowhere in its discussion of the proportionality rule does the telegram refer to the responsibility of the defending force or otherwise indicate that the proportionality rule excludes harm to human shields.

In short, the telegram states that involuntary shields \textit{retain} their protection under the precautions rule and that an attack that satisfies the precautions rule is necessarily not \textit{indiscriminate}. In contrast, the telegram never says that involuntary shields \textit{lose} their protection under the proportionality rule or that an attack that satisfies the precautions rule is necessarily not \textit{disproportionate}. Simply put, the telegram provides no legal support for the

\begin{flushright}
132. \textit{Id.} at 2063.
133. DoD MANUAL, supra note 1, ¶ 5.12.3.3 n.315.
134. U.S. Comments, supra note 37, at 2057, 2059.
135. \textit{Id.} at 2063–64.
\end{flushright}
Manual’s position that civilians used as involuntary shields retain their protection under the precautions rule but lose their protection under the proportionality rule.

In his 1990 article, Parks asserts that “[u]nder the customary law of war, casualties resulting from a defender’s use of the civilian population as concealment or cover from attack of legitimate military objectives are not the responsibility of the attacker so long as he has exercised ordinary care.”136 Parks repeats this assertion throughout his article.137 Remarkably, Parks cites only two sources that directly support his assertion. The first source is a quotation from the 1924 edition of Air Power and War Rights by James Spaight, a distinguished scholar and lawyer for the British Air Ministry:

[A]s a belligerent cannot allow himself to be prejudiced because the enemy locates . . . [military] objectives in places where they cannot be destroyed without incidental injury to civilians, he is not responsible for the resulting damage provided all due care is taken to prevent unnecessary injury.138

Parks’ reliance on this quotation is curious since, in the 1933 edition of the very same book, Spaight writes that “[i]f a military objective is situated in such a densely populated neighborhood, or if the circumstances of the case are otherwise such that any attack upon it from the air is likely to involve a disastrous loss of non-combatant life, aircraft are bound to abstain from bombardment.”139 It seems that Spaight’s considered view was that attackers remain bound by the proportionality rule despite the misconduct of defenders.

The second source that Parks cites as direct support for his assertion is the following passage from the 1976 Air Force Pamphlet discussed earlier:

The failure of states to segregate and separate their own military activities, and particularly to avoid placing military objectives in or near populated areas and to remove such objectives from populated areas, significantly and substantially weakens effective protection for their own population. A party to a conflict which places its own citizens in positions of danger

136. Parks, supra note 115, at 162.
137. See, e.g., id. at 163, 168, 176, 178, 182.
138. Id. at 162 (quoting James Spaight, Air Power and War Rights 244 (1st ed. 1924)).
by failing to carry out the separation of military activities from civilian activities necessarily accepts, under international law, the results of otherwise lawful attacks upon valid military objectives in their territory.\(^{140}\)

This passage provides no support for Parks' assertion. The pamphlet states that a defender's placement of military objectives in or near a populated area weakens effective protection for their own population. The pamphlet does not state that a defender's misconduct weakens legal protection for its own population. Similarly, the pamphlet states that a party that places its own citizens in danger accepts the results of otherwise lawful attacks upon valid military objectives. Evidently, an attack expected to cause harm to civilians out of all proportion to the anticipated military advantage is not otherwise lawful. Nowhere does the pamphlet state that an otherwise unlawful attack is lawful if the civilians it is expected to kill are human shields.

On the contrary, the Air Force pamphlet observes that civilian casualties may occur in armed conflict due to several factors, including the fact that civilians may be "used unlawfully in an attempt to shield military objectives from attack."\(^{141}\) In the very same paragraph, the pamphlet then explains that

Attacks are not prohibited against military objectives even though incidental injury or damage to civilians will occur, but such incidental injury to civilians or damage to civilian objects must not be excessive when compared to the concrete and direct military advantage anticipated. Careful balancing of interests is required between the potential military advantage and the degree of incidental injury or damage . . . \(^{142}\)

In short, the pamphlet applies the proportionality rule to all incidental injury to civilians, with no exception for civilians used as involuntary shields.

Finally, Parks asserts throughout his article that international law traditionally held defenders "responsible" for collateral harm to civilians.\(^{143}\) Parks appears to rest his assertion on the historical fact that, for centuries, international law did not clearly prohibit attackers from inflicting extensive collateral harm on civilians, paradigmatically during siege warfare, but only

\(^{140}\) Parks, supra note 115, at 162 (quoting AFP 110-31, supra note 23, at 5-13).

\(^{141}\) AFP 110-31, supra note 23, at 5-10.

\(^{142}\) Id.

\(^{143}\) See, e.g., Parks, supra note 23, at 4, 51, 55, 59, 62.
from attacking undefended areas. Parks goes on to claim that Protocol I illegitimately “shifted” responsibility from defenders to attackers. 144

In my view, Parks’ legal argument rests on a conceptual mistake. As the Manual itself recognizes, the law governing the conduct of hostilities is prohibitive rather than permissive. 145 It follows that the absence of a clear prohibition should never be confused for an affirmative authorization. Sadly, there was a time when international law did not clearly prohibit rape, enslavement, or the murder of prisoners. It hardly follows that international law authorized such conduct or held defenders “responsible” for such conduct. Similarly, the fact that the proportionality rule was slow to crystalize does not entail that customary law authorized attackers to inflict expected harm out of all proportion to anticipated advantage or absolved attackers of “responsibility” for such disproportionate harm. We should not interpret the slow and halting advance of international law as a positive endorsement of the status quo ante. It seems that Parks’ argument, repeated almost verbatim in the Manual, is legally unsound. As we shall see, this argument is logically invalid as well.

2. Logic

To recall, the Manual claims that a defender who employs human shields assumes responsibility for their injury and concludes that an attacker who expects to kill many human shields in pursuit of a small military advantage does not violate the proportionality rule. Simply put, the DoD’s conclusion is a non sequitur. Of course, defenders who use human shields are responsible for the foreseeable harm that they occasion. It simply does not follow that attackers who kill human shields are not responsible for the foreseeable harm that they inflict and may therefore inflict foreseeable harm out of all proportion to the military advantage they anticipate. In the context of war, attributing responsibility is not a zero-sum game.

Return to the scenario with which we began. No doubt, the combatant has acted wrongfully, even criminally, by using the residents as involuntary shields. But now the choice is yours: to kill the residents or to spare them. If you choose to kill the residents then you cannot deny responsibility for your choice. The combatant is responsible for his choice and you are responsible for yours. The combatant is wrong to use the residents as invol-

144. See, e.g., id. at 112.
145. DoD MANUAL, supra note 1, ¶ 1.3.3.1.
unitary shields and you would be wrong to kill the residents simply to eliminate the combatant.

Suppose that a bank robber takes a bank teller hostage and uses her to shield his escape. You are a police officer and may lawfully kill the bank robber to prevent his escape. However, if you shoot at the bank robber then you will almost certainly kill the hostage as well. If you shoot at the bank robber and kill the hostage, then no doubt the robber (assuming he survives) will be held criminally responsible for her death. After all, he put her in harm’s way. But surely you may also be held criminally responsible for her death. After all, you shot her. Perhaps you can convince a court that you did not act recklessly, that the risk of killing the hostage, though substantial, was justifiable in light of the danger posed by the bank robber. But surely you will convince no one that, so long as you tried your best not to shoot the hostage, you had no obligation to weigh the risk of killing her against the need to stop the robber. The robber put her in harm’s way but, ultimately, her life was in your hands.

In his 1990 article, Parks writes that “[p]lacing civilians in proximity to a military position that is likely to be attacked with the intent of shielding that object from attack differs little from lining up those same civilians and executing them by firing squad; the same premeditation is required.”146 Certainly, those who line up civilians before a firing squad are responsible for their deaths. Nevertheless, the members of the firing squad who shoot the civilians are also responsible for their deaths. The guilt of the former does not entail the innocence of the latter.

Parks begs the question when he writes that “the illegal act . . . is the crime that places innocent civilians at risk, while attack of a lawful target is a legitimate act authorized by the law of war.”147 Indeed, using human shields is an illegal act and a war crime. However, attack of a lawful target is not a legitimate act authorized by the law of war if such an attack is expected to inflict harm on civilians that would be excessive in relation to the military advantage anticipated. In the quoted passage, Parks seems to as-

146. Parks, supra note 115, at 163. As an aside, note that this sentence is literally false. If the defenders place civilians in proximity to a military position with the intent of shielding that object from attack then they do not intend for the civilians to be killed. On the contrary, they intend for no attack to take place and for both the object and the civilians to remain unharmed. If the defenders are aware that the position is likely to be attacked then they cause the deaths of the civilians with extreme recklessness, not with premeditation.

147. Id. at 163.
sume his conclusion, namely that expected harm to human shields cannot render attack of a lawful target an illegitimate act prohibited by the law of war.

Finally, Parks writes the following:

Attack of a military objective, wherever located, is lawful. While the number of civilian casualties that occur are the result of that attack, the attack is not necessarily the cause of those casualties, nor may they necessarily be attributable to the attacker. The approach under discussion suggests that "but for the attack, these civilian losses would not have occurred; therefore the attacker is responsible." This approach would make any attack on any target, wherever located, illegal, notwithstanding the actions of the defender.\textsuperscript{148}

Every sentence of this passage is incorrect. First, attack of a military objective, wherever located, is lawful \textit{only if} it is not expected to inflict harm on civilians that would be excessive in relation to the military advantage anticipated. Second, if civilian casualties are the result of an attack then, by definition, the attack \textit{is} necessarily the cause of those casualties. That is what the words "cause" and "result" mean. Third, if "but for the attack, these civilian losses would not have occurred" then of course the attacker is \textit{causally} responsible for those losses (as is the defender). In contrast, the attacker is \textit{criminally} responsible for those losses only if the expected losses were excessive in relation to the anticipated advantage. For its part, the defender is criminally responsible for using human shields whether harm results or not.\textsuperscript{149} Finally, the approach Parks rejects would not make any attack on any target, wherever located, illegal, if it is expected to harm civilians. Instead, on this approach, an attack on a legitimate target is illegal only if the expected harm to civilians would be excessive in relation to the anticipated military advantage.

D. Deterrence

The \textit{Manual} also claims that "[i]f the proportionality rule were interpreted to permit the use of human shields to prohibit attacks, such an interpreta-

\textsuperscript{148} \textit{Id.} at 177.
tion would perversely encourage the use of human shields.\textsuperscript{150} Put the other way around, if the proportionality rule is interpreted to exclude expected harm to human shields, such an interpretation would discourage the use of human shields. Parks makes similar claims throughout his 1990 article.\textsuperscript{151} This argument rests on a series of legal, factual, and logical mistakes.

First, this argument falsely assumes that individual civilians enjoy specific legal protections unless and for such time as stripping them of some legal protections might yield desirable consequences. On the contrary, individual civilians enjoy general legal protection unless and for such time as they take a direct part in hostilities.\textsuperscript{152} It is a truism that the law of war seeks to “alleviat[e] as much as possible the calamities of war.”\textsuperscript{153} It hardly follows that the law of war is some crude exercise in rule-consequentialism.\textsuperscript{154} Parties should always strive to reduce overall suffering, but never at the expense of individual civilians entitled to legal protection.

For example, the law of war does not permit terroristic attacks directed against civilians even when such terror would hasten the end of the war. Nor does the law of war permit attacking civilians in order to leave irregular combatants nowhere to hide. Similarly, even if excluding expected harm to involuntary shields from the proportionality rule would discourage the future use of involuntary shields, it simply does not follow that the law of war should deny those civilians who are used as involuntary shields legal protection under the proportionality rule. Civilians lose their legal protection only when they choose to directly participate in hostilities, not whenever dictated by some utilitarian calculus.

Importantly, it is a State’s conduct, not its interpretation of the proportionality rule as such, that affects a defender’s incentives to use human shields. In order to discourage the use of human shields in the way the Manual suggests, the United States would have to order our forces to knowingly kill civilian men, women, and children—forced against their will or used without their consent as involuntary human shields—whose deaths

\begin{itemize}
\item \textsuperscript{150} DOD MANUAL, supra note 1, ¶ 5.12.3.3.
\item \textsuperscript{151} See Parks, supra note 115, at 163, 177, 181.
\item \textsuperscript{152} See CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, supra note 6, at 19; Protocol I, supra note 18, art. 51.
\item \textsuperscript{153} Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight [St. Petersburg Declaration], Nov. 29/Dec. 11, 1868, 138 Consol. T.S. 297, 18 Martens Nouveau Recueil (ser. 1) 474.
\item \textsuperscript{154} Roughly, rule-consequentialism is the view that we morally ought to follow those rules that, were they generally followed, would produce the greatest aggregate wellbeing across all affected persons. See, e.g., 1 DEREK PARFIT, ON WHAT MATTERS 375 (2011).
\end{itemize}
would ordinarily be considered excessive in relation to the concrete and
direct military advantage anticipated. In blunt terms, the Manual proposes
that we kill more civilians now so we will have to kill fewer civilians later.

As far as I am aware, there is no empirical evidence that if we exclude
civilians used as human shields from the proportionality rule then we will
end up killing fewer civilians overall. True, if attackers disregard harm to
human shields then defenders may use fewer civilians as human shields; on
the other hand, attackers will kill almost all of those civilians whom de-
defenders nevertheless use as human shields. The number used may be smaller,
but the proportion killed will be greater. Conversely, if attackers apply
the proportionality rule to human shields then defenders may use more
civilians as human shields; on the other hand, attackers will only kill some
of the civilians who are in fact used as human shields. The number used
may be greater, but the proportion killed will be smaller. Absent empirical
evidence that the difference in the number used will offset the difference in
the proportion killed, the DoD’s position seems to rest entirely on a priori
speculation.

Of course, the proportionality rule prohibits attacks expected to kill ci-
vilians that are based on mere speculation that the long-term benefits will
outweigh the short-term costs. Instead, the proportionality rule compares
expected harm to civilians only to the concrete and direct military advantage
anticipated. According to the ICRC, “the advantage concerned should be
substantial and relatively close, and . . . advantages which are hardly percep-
tible and those which would only appear in the long term should be disre-
garded.”155 The Manual takes a more expansive view (a topic for another
day), but concedes that, under the proportionality rule, “the military ad-

tantage may not be merely hypothetical or speculative.”156 It seems illogical
to deny civilians protection under the proportionality rule based on the
very kind of speculation that the rule itself rejects.

Indeed, the DoD’s a priori prediction that disregarding expected harm
to involuntary shields will dramatically reduce the use of involuntary shields is
highly implausible. Presumably, defenders heedless of law and morality
will use involuntary shields if and only if the expected benefits to defenders
outweigh the expected costs to defenders. By disregarding harm to invol-
untary shields, attackers deprive defenders of one potential benefit of using
human shields, namely temporary avoidance of attack. The question then

155. PROTOCOL I COMMENTARY, supra note 22, ¶ 2209.
156. DoD Manual, supra note 1, ¶ 5.12.5.
becomes whether the other expected benefits of using involuntary shields outweigh the expected costs of using involuntary shields.

Importantly, it is not ordinarily costly for a combatant to take refuge in a residential building, for a group to establish a command center in a hospital, or for a unit to fire rockets from a schoolyard. In each such case, defenders use civilians as involuntary shields at little cost to themselves. It follows that if ruthless defenders expect any significant benefit from using civilians as involuntary shields then they will do so irrespective of the legal position of the attacking force. For example, if such defenders expect that the killing of involuntary shields by attackers will redound to the defenders’ broader strategic advantage—by, for instance, gaining them new recruits or by politically isolating attackers—then defenders will continue to use involuntary shields when it is not costly to do so. Significantly, since only the defenders’ subjective expectations affect their behavior, it does not matter whether they are in fact likely to gain the advantage that they expect.

In an earlier exchange, Charles Dunlap notes that taking and maintaining hostages is often quite costly, such that if harm to hostages is excluded from the proportionality rule then the costs of taking hostages would outweigh the benefits of taking hostages. Of course, most involuntary shields are not hostages who need to be fed, clothed, washed, hidden, and regularly moved (think again of the apartment residents, the hospital patients, and the school children in the previous examples). In addition, many hostages are held for ransom rather than for use as human shields. Finally, many hostages are taken from the attacker’s political community; attackers may therefore refrain from attack not for legal reasons but for emotional, political or ethical reasons. It is therefore doubtful that excluding harm to hostages from the proportionality rule will reduce the number of hostages taken by defenders enough to offset the number of hostages killed by attackers.

In any event, as we have seen, such utilitarian considerations are legally beside the point. The law of war protects each individual civilian unless and for such time as he or she directly participates in hostilities. There is no legal basis for stripping individuals of their protection under the propor-

---

tionality rule in the hope that the long-term benefits to others may out-
weigh the immediate costs to them. Nor, as we have seen, is there any fac-
tual or logical basis for doing so.

E. Fairness

Finally, the DoD claims that

If the proportionality rule were interpreted to permit the use of human
shields to prohibit attacks, such an interpretation would . . . allow viola-
tions by the defending force to increase the legal obligations on the at-
tacking force.158

Similarly, in his 1990 article, Parks writes that "an attacker facing a target
shielded from attack by civilians . . . is [not] obligated to assume any addi-
tional responsibility as a result of the illegal acts of the defender."159

In fact, violations by the defending force do not "increase" the legal
obligations on the attacking force, but instead trigger the ordinary legal ob-
ligation not to inflict excessive incidental harm on civilians. Evidently, de-
fending forces trigger this obligation whenever they locate their personnel
and equipment near civilians, whether or not they intend to thereby shield
their personnel and equipment from attack and whether or not they fail to
take feasible precautions against the effects of attacks. When this obligation
is triggered, attackers are free to grumble but they must obey.

Similarly, Parks' reference to "additional responsibility" is misplaced.
Both the responsibility to exercise reasonable precautions and the respon-
sibility not to inflict excessive incidental harm on civilians are basic respon-
sibilities that the law of war imposes on all attacking forces. Naturally, both
responsibilities are triggered if, and only if, civilians are near military objec-
tives. Importantly, these general responsibilities are triggered whether civili-
ans are near military objectives by chance or by force, and whether de-
fenders are fulfilling or breaching their own legal responsibilities.

Perhaps the DoD means that it is unfair for defending forces to inten-
tionally trigger the legal obligations of the attacking force, through unlawful
conduct, as a means of obtaining tactical advantage. Put more simply, it
seems unfair for defenders to profit from their wrongdoing. Indeed it is.
However, it does not follow that attacking forces may deprive defending

158. DoD Manual, supra note 1, ¶ 5.12.3.3.
159. Parks, supra note 115, at 163.
forces of such unfair advantages by killing involuntary shields out of all proportion to the military advantage anticipated from an attack.

War, like other parts of life, is often unfair. Killing involuntary shields shifts the unfair burdens imposed on the attacking force, not onto the defending force that imposed them, but onto the latter's civilian victims. We cannot correct but can only compound the unfairness of war by killing civilians who have done nothing to forfeit their legal rights. Instead, we should annul the unfair advantages gained through the use of involuntary shields by prosecuting those who use them for war crimes. We should not, in effect, punish civilians for war crimes committed against them.160

V. CONCLUSION

As its authors remind its users, the Manual "is not a substitute for the careful practice of law." In my view, the careful practice of law will often require cautioning commanders and warfighters against following the Manual's provisions on target selection, precautions in attack, and proportionality as it concerns human shields. Legal advisors are duty-bound to offer professional, candid, and independent counsel regarding, inter alia, the international law of war. If a legal advisor determines that military operations that comply with the Manual nevertheless violate international law then it is his or her duty to inform combatants of the discrepancy and to advise the legally safer course of action. If combatants find such advice confusing or unsatisfying then they should address their concerns to the General Counsel of the DoD.

The Manual "does not necessarily reflect the views of any other department or agency of the U.S. Government or the views of the U.S. Government as a whole." It follows that the Manual cannot be assumed to reflect U.S. opinio juris or to generate customary international law. Nevertheless, states like Saudi Arabia and Sri Lanka may cite the Manual to justify their wartime conduct, particularly with respect to the killing of civilians forced to serve as involuntary human shields. If they do so then the U.S. State Department may have to intervene and clarify the U.S. position.

160. Cf. Schmitt, supra note 108, at 301 (observing that "equalizing the fighting position of belligerents is not an underlying purpose of LOIAC").
161. DoD MANUAL, supra note 1, ¶ 1.1.2.
162. Id. ¶ 1.1.1.
Finally, the *Manual* "does not . . . preclude the Department from subsequently changing its interpretation of the law."\(^{164}\) In my view, the Department should change its interpretation of the law without delay. Every day that the *Manual* remains unchanged increases the risk that it will be relied upon by the U.S. military, by the U.S. Central Intelligence Agency, or by foreign States. If that happens then civilian men, women, and children will lose their lives in violation of international law. Alternatively, the law of war may lose its moral credibility in the eyes of our armed forces.

When the President of the United States assures the American people and the people of the world that the United States obeys the law of war—even in covert operations—those words should mean something. Those words should mean that the United States selects targets so as to minimize loss of civilian life; that the United States takes precautions to avoid harm to civilians, even at reasonable risk to attacking forces; and that the United States will not knowingly kill civilians except when justified by the concrete and direct military advantage anticipated. So long as the *Manual* remains unchanged, such assurances will mean little or even nothing. The world will not know whether the President refers to the international law of war or to the law of the *Manual*. Whenever civilians are killed in U.S. operations the world will wonder which law we followed. Many will assume the worst. In such ways, the *Manual* undermines the international legitimacy of U.S. military action. In this sense, the *Manual* is a self-inflicted act of "lawfare."\(^{165}\)

---

Government of Sri Lanka should immediately use its diplomatic channels to clear its name with the US Department of State based on the deliberations found in the 1204-page DOD Manual. . . Using the language of the DOD Manual when in discourse with state department officials is the first move: after all, it is their policy document on Law of War."

164. DOD MANUAL, supra note 1, ¶ 1.1.1.

165. For the intended meaning and unintended use of the term, see Charles J. Dunlap, Jr., *Lawfare Today . . . and Tomorrow*, 87 INTERNATIONAL LAW STUDIES 315 (2011).
Common Article 1 to the Geneva Conventions and the obligation to prevent international humanitarian law violations

Knut Dörmann and Jose Serralvo*
Dr Knut Dörmann is Head of the Legal Division at the International Committee of the Red Cross (ICRC). Jose Serralvo is legal adviser in the Legal Division at the ICRC.

Abstract
Common Article 1 to the four Geneva Conventions lays down an obligation to respect and ensure respect for the Conventions in all circumstances. This paper focuses on the second part of this obligation, in particular on the responsibility of third States not involved in a given armed conflict to take action in order to safeguard compliance with the Geneva Conventions by the parties to the conflict. It concludes that third States have an international legal obligation not only to avoid encouraging international humanitarian law violations committed by others, but also to take measures to put an end to on-going violations and to actively prevent their occurrence.

Keywords: Common Article 1 to the Geneva Conventions, ensuring respect, obligation *erga omnes*, compliance, third States’ responsibility, Stockholm Conference, treaty interpretation, preventing IHL violations, stopping IHL violations, prevention, Arms Trade Treaty.
The importance of compliance

Contemporary armed conflicts – such as those in Syria, the Central African Republic and South Sudan, to name just a few – continue to be marked by enormous human suffering. They also illustrate how complex armed violence has become nowadays. Despite the emergence of new actors of violence, and new means and methods of warfare, all of which may put existing international humanitarian law (IHL) rules to the test, IHL continues to provide an adequate framework to attenuate the effects of armed conflict and to establish a judicious balance between the principles of humanity and military necessity.\(^1\) Treaty and customary law provisions set limits to the waging of war, but the single biggest challenge facing IHL today lies in persuading parties to the conflict to comply with the rules by which they are bound. Violations of the most fundamental and uncontroversial rules remain a sad reality.\(^2\) Stricter compliance with existing IHL rules would considerably improve the plight of persons affected by armed conflicts.\(^3\) Thus, there is a pressing need to generate respect for the law and, as one important avenue in this context, to re-emphasize and clarify the extent to which, as provided by common Article 1 to the four Geneva Conventions (CA I), as well as by Article 1(1) of Additional Protocol I (AP I), the High Contracting Parties thereto are bound to “respect and ensure respect” for their provisions “in all circumstances”.

The obligation to respect the Geneva Conventions means that a State must do everything it can to guarantee that its own organs abide by the rules in question.\(^4\) In essence, this part of the provision reaffirms the basic principle of *pacta sunt servanda*, codified in Article 26 of the Vienna Convention on the Law of Treaties. In the case of a non-international armed conflict, the obligation to respect also binds organized armed groups, in accordance with Common Article 3. Indeed, compliance with IHL is the primary responsibility of the parties to a conflict. However, CA I goes one step further by introducing an undertaking to ensure respect in all circumstances, which, in turn, consists of an internal and an external component. The internal component implies that each High Contracting Party to the Geneva Conventions must ensure that the Conventions are respected

---

1 See the report presented by the International Committee of the Red Cross (ICRC) to the 31st International Conference of the Red Cross and Red Crescent, *Strengthening Legal Protection for Victims of Armed Conflicts*, ICRC, Geneva, October 2011, p. 4.

2 Even the most longstanding IHL obligation, which was at the heart of the early treaty IHL, *i.e.* the delivery of impartial healthcare in armed conflict, is affected by this lack of respect vis-à-vis existing rules. See ICRC, *Healthcare in Danger: Making the Case*, August 2011, available at: www.icrc.org/eng/assets/files/publications/icrc-002-4072.pdf.

at all times not only by its armed forces and its civilian and military authorities, but also by the population as a whole.\textsuperscript{5} The existence of this internal obligation, as well as the possibility to hold States legally responsible in case of failure to comply with it, is widely accepted. The external component postulates that third States not involved in a given armed conflict – and also regional and international organizations\textsuperscript{6} – have a duty to take action in order to safeguard compliance with the Geneva Conventions, and arguably with the whole body of IHL, by the parties to the conflict.

The purpose of this article is to cast some light upon this external component, which some authors have described as being beset by uncertainty.\textsuperscript{7} In particular, emphasis will be placed on the nature and extent of the obligations of each High Contracting Party to the Geneva Conventions to ensure respect by the other High Contracting Parties, whether they are a party to the conflict or not.\textsuperscript{8} If compliance with existing IHL constitutes the key element for averting current humanitarian problems during armed conflict, there is then a need to elucidate the extent of this obligation. For instance, in a conflict in which a State A systematically mutilates civilians from a State B, must a neutral State C endeavour to stop such mutilations? In a situation of occupation in which a State A prevents the occupied territory of a State B from receiving humanitarian assistance, what are the responsibilities of a non-belligerent State C with close diplomatic ties to State A? Is it lawful for a State C to sell weapons to a State A, if it knows that they are going to be used to commit serious IHL violations in a conflict against a State B? CA 1 is a sound basis for dealing with these matters.

By construing the scope of CA 1, this article will demonstrate that third States – that is, States not taking part in an armed conflict – have an international legal obligation to actively prevent IHL violations. First, it will examine the historical background of the obligation to ensure respect, in particular by revisiting the \textit{travaux préparatoires} to the Geneva Conventions of 1949. Second, it will focus on an array of subsequent practice by States, intergovernmental organizations and international tribunals, supporting the view that third States indeed have a duty to ensure compliance with IHL, even in conflicts to which they are not a party. After having evinced the existence of this external

---


\textsuperscript{6} Adam Roberts considers that if States have an obligation to ensure respect, then regional and global international organizations are also bound by this very same obligation, since they are themselves composed of States. See Adam Roberts, “Implementation of the Laws of War in Late 20th Century Conflicts”, in Michael N. Schmitt and Leslie C. Green (eds), \textit{The Law of Armed Conflict: Into the Next Millennium}, International Law Studies, Vol. 71, Naval War College, Newport, 1998, p. 365.

component of the obligation, the article will assess its exact nature. In that sense, it will frame CA 1 within the context of an obligation of due diligence – as opposed to an obligation of result – and will briefly enumerate a series of measures available to States in order to comply therewith. Lastly, the article will look at the type of action that CA 1 requires from High Contracting Parties to the Geneva Conventions, or prohibits them from taking. This last part will emphasize the role that CA 1 can play in delineating a preventive approach to IHL violations. For these purposes, the recently adopted Arms Trade Treaty will be used as a case study.

Historical background of the obligation to ensure respect by others

Article 25 of the 1929 Geneva Convention on the Amelioration of the Condition of the Wounded and Sick in Armies in the Field and Article 82 of the 1929 Geneva Convention on the Treatment of Prisoners of War already established that both texts “shall be respected by the High Contracting Parties in all circumstances”. These provisions have been unanimously read as imposing, for the first time, the obligation to abide by the rules of the Conventions regardless of the behaviour of other parties.9 Apart from their unprecedented character within the law of treaties,10 Articles 25 and 82 of the 1929 Geneva Conventions laid down the foundations of what is now known as the principle of non-reciprocity11 – in other words, that reciprocity may not be invoked to disregard IHL obligations in case the adversary violates the law. If the 1929 Geneva Conventions marked a milestone in the efforts to safeguard compliance with IHL, CA 1 to the four Geneva Conventions of 1949 went a step further by asserting that “the High Contracting Parties undertake to respect and to ensure respect for the [Geneva Conventions] in all circumstances”. Three major diverging features need to be highlighted between CA 1 and its 1929 predecessors:

1. First and foremost, CA 1 introduced the obligation to “ensure respect” for the Geneva Conventions. Several of the numerous implications of this new commitment will be discussed below.


10 Note that, under the law of treaties, a material breach of a treaty by one of the parties allows the others to terminate the treaty or to suspend its operation in whole or in part. Article 60(5) of the 1969 Vienna Convention on the Law of Treaties recognizes the exception to this rule, anticipated by the 1929 Geneva Conventions, by providing that this regime “do[es] not apply to provisions relating to the protection of the human person contained in treaties of a humanitarian character, in particular to
2. Second, unlike in 1929, when the obligation to respect in all circumstances was placed within the chapters dealing with the issue of execution at the very end of the Conventions, the 1949 Diplomatic Conference decided to place the more far-reaching obligation of CA 1 right at the beginning of all four Geneva Conventions. Such a decision should be seen as anything but trivial, in terms both of its purpose and of its imperative nature.\(^{12}\)

3. Third, CA 1 is written in the active voice ("The High Contracting Parties undertake to respect and to ensure respect"), whereas its 1929 counterparts resorted to the passive voice ("shall be respected by the High Contracting Parties"). Regardless of whether the use of a particular grammatical construction entails any legal value, the wording of CA 1 helps to emphasize the system of protection underpinning the Geneva Conventions, and hence its interpretation.

The common Articles to the Geneva Conventions reflect matters that the drafters deemed significant enough "to merit emphasis through repetition".\(^{13}\) It is reasonable to assume that CA 1 goes beyond the mere obligation to respect the Geneva Conventions at the domestic level. After all, the above-mentioned customary principle *pacta sunt servanda* already acknowledges that any State ratifying a particular treaty is bound to respect it in good faith. If CA 1 represents such a breakthrough in the development of IHL, it is not because it reiterates an already existing and uncontroversial rule of public international law but rather due to its unprecedented creation of a legal obligation for each State to ensure respect towards the international community as a whole.\(^{14}\) This is what can be deduced from a joint analysis of the *travaux préparatoires* and the subsequent application of CA 1 for over sixty years.

Before looking back at the inception of the Geneva Conventions, it is necessary to highlight that the *travaux préparatoires* are to be seen as a supplementary means of interpretation,\(^{15}\) contrary to the ulterior behaviour of States in the application of a treaty, which constitutes a primary source in the analysis of conventional obligations.\(^{16}\) Nevertheless, taking into consideration

\(^{12}\) See Fateh Azzam, "The Duty of Third States to Implement and Enforce International Humanitarian Law", *Nordic Journal of International Law*, Vol. 66, 1997, p. 72: "Article 1 … is not preambular or introductory, it is an active provision of the Conventions and Protocol and indeed, its placement at the very beginning of both is an indication of its imperative nature." See also Jean Pictet (ed.), *Commentary: IV Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, 1958, p. 15.


\(^{15}\) Vienna Convention on the Law of Treaties, Art. 32.


Si le recours aux travaux préparatoires souligne le souci de connaître cette volonté dans la phase de gestation du traité, recourir à l'examen de l'application et de l'exécution de ce dernier souligne le
that—as stated above—some authors have deemed the undertaking to ensure respect by others to be a norm surrounded by uncertainty, a study of both the origin and practice of this obligation will shed further light upon the nuances of the rule.

Travaux préparatoires

According to François Bugnion, the travaux préparatoires to the Geneva Conventions are not conclusive when it comes to construing the scope of CA 1. He asserts that both the internal and external aspects of the duty to ensure respect were put forward and that the Diplomatic Conference of 1949 did not find it necessary to decide between them. The formulation retained would permit both interpretations. Frits Kalshoven has gone one step further by stating that nothing in the travaux préparatoires justifies an interpretation of CA 1 whereby third States have an international legal obligation to ensure respect for the Geneva Conventions in conflicts to which they are not a party.

In his analysis of the drafting history of CA 1, Kalshoven concluded that the drafters did not intend an interpretation whereby the phrase “to ensure respect” implied that each High Contracting Party undertook to ensure respect by all other parties. In his view, there is “simply nothing to suggest that the authors of the proposed text, with Claude Pilloud as the key figure among them, were thinking along those lines.” Kalshoven considers that CA 1 simply sought to address the issue of implementation of the Geneva Conventions in the event of non-international armed conflict (NIAC)—that is, to ensure that the non-State party to a NIAC also respects the basic precepts of IHL.

The admittedly scarcely documented drafting history can also be understood differently. The obligation to ensure respect was first introduced in the opening articles of each one of the Draft Revised or New Conventions for the Protection of War Victims submitted by the ICRC to the Stockholm International Conference of the Red Cross in 1948. The ICRC established the drafts with the assistance of government experts, National Red Cross Societies and other humanitarian associations. The final text, presented in the form of a booklet, contained both the proposed articles and details on the meaning and justification of each provision. The exact proposed wording of CA 1 was the following:

The High Contracting Parties undertake, in the name of their peoples, to respect, and to ensure respect for the present Convention in all circumstances.

18 F. Kalshoven, above note 9, pp. 3–61.
20 Ibid.
Next to this text, the ICRC introduced a series of remarks. The booklet was made available to all National Red Cross Societies and governments participating at the Stockholm Conference.\textsuperscript{24} Due to its importance to understanding the original meaning of the obligation to ensure respect, it is worth reproducing the remarks made to CA 1 in their entirety (emphasis added):

The ICRC believes that this Article, \textit{the scope of which has been widened}, should be placed at the head of the Convention. The new wording covers three points:

1. The undertaking subscribed to by High Contracting Parties to respect the Convention in all circumstances.
2. The undertaking subscribed to by the High Contracting Parties to ensure respect for the Convention in all circumstances.
3. A formal declaration stating that the two above undertakings are subscribed to by Governments in the name of their peoples.

Re (1) This stipulation corresponds to Art. 25, Sec. 1, of the 1929 Convention. Re (2) The ICRC believes it necessary to stress that if the system of protection of the Convention is to be effective, the High Contracting Parties cannot confine themselves to implementing the Convention. \textit{They must also do everything in their power to ensure that the humanitarian principles on which the Convention is founded shall be universally applied}. Re (3) By inviting the High Contracting Parties to make formal declaration of their undertaking, in the name of their peoples, the ICRC aims at associating the peoples themselves with the duty of ensuring respect for the principles on which the present Convention is founded, and of implementing the obligations which result therefrom. Another advantage of the present wording will be to facilitate the implementing of the present Convention, especially in case of civil war.\textsuperscript{25}

Kalshoven argues that the authors used the word “universal” as a way to ensure compliance with the Geneva Conventions by all parties to a NIAC.\textsuperscript{26} He submits that “for a concept belonging to the realm of international relations to figure without explanation between two elements relating to the domestic level would be very strange indeed”.\textsuperscript{27} Kalshoven also considers that

precious little had ... remained of the original motives behind ... the new draft Article 1. For its authors, its main \textit{raison d’être} now appeared to lie in getting populations involved in the process of creating and maintaining respect for the principles embodied in the Conventions, thus binding them to such respect even in time of civil war or non-international armed conflict.\textsuperscript{28}

\textsuperscript{24} Ibid., n. 2.

\textsuperscript{25} Ibid., n. 2.

\textsuperscript{26} Ibid., n. 2.

\textsuperscript{27} Ibid., n. 2.

\textsuperscript{28} Ibid., n. 2.
The following elements, it is submitted, may also prompt a different understanding of the underlying intent:

1. The draft Article 2 presented to the Stockholm Conference by the ICRC already dealt with the issue of civil war (in paragraph 4), explicitly stating the binding nature of the obligation to respect for IHL for all parties to a NIAC; and draft Article 1, by maintaining the notion of "to respect the Conventions in all circumstances", coupled with a statement in draft Article 2 confirming that the clausula si omnes contained in earlier IHL treaties would not govern the relations of parties to an armed conflict (in paragraph 3), restated the principle of non-reciprocity. At the same time, the remarks made by the ICRC with regard to CA 1 (see above) began by spelling out that the scope of this provision was wider than that of its equivalents in the 1929 Geneva Conventions. Since both the principle of non-reciprocity and the issue of civil war were being dealt with elsewhere, one must presuppose that this enlarged scope mainly referred to the obligation to ensure respect universally.

2. The third paragraph of the remarks made by the ICRC already dealt with the issue of non-international armed conflict. Thus, the second paragraph thereof must have a different scope.

3. The ordinary meaning of the term “universal” used in the ICRC remarks is particularly univocal and one can comfortably assert that, at least in the domain of international law, it means the very opposite of domestic. Scholars like Eric David agree with the reading that a universal application of CA 1 can obviously not be restricted to a national level. The Stockholm text and the related remarks may therefore well be read with such a wider understanding.

The travaux préparatoires of the 1949 Diplomatic Conference show that there was very little discussion on the issue of CA 1. Only Italy, Norway, the United States, the ICRC and France took the floor during the deliberations at the Special Committee. Mr Maresca, representing Italy, pointed out that the obligation to ensure respect was “either redundant or introduced a new concept into international law”. As shown above, there are good reasons to believe that the latter is true – otherwise, if it would merely have been redundant, one might have expected a deletion. The delegates

---

29 Paragraphs 3 and 4 of draft Article 2 stated the following:

Should one of the Powers in conflict not be party to the present Convention, the Powers who are party thereto shall, nevertheless, be bound by it in their mutual relations.

In all cases of armed conflict which are not of an international character, especially cases of civil war, colonial conflicts, or wars of religion, which may occur in the territory of one or more of the High Contracting Parties, the implementing of the principles of the present Convention shall be obligatory on each of the adversaries. The application of the Convention in these circumstances shall in no wise depend on the legal status of the parties to the conflict and shall have no effect on that status.
from Norway and the US highlighted that the object of CA 1 was to ensure respect “by the population as a whole”, without elaborating on the issue.\textsuperscript{33} After that, Mr Pilloud, on behalf of the ICRC, pointed out that

in submitting its proposals to the Stockholm Conference, the International Committee of the Red Cross emphasized that the Contracting Parties should not confine themselves to applying the Conventions themselves, but should do all in their power to see that the basic humanitarian principles of the Conventions were universally applied.\textsuperscript{34}

None of the delegates opposed this statement, nor did they raise any issues regarding their accord—or discord—with the statements made by Norway, the US and the ICRC.\textsuperscript{35} It may therefore be assumed that the universal application of a treaty should not be restricted to the domestic level.\textsuperscript{36} Since a draft with clarifying remarks had been distributed to all the participants—and taking into consideration that a straightforward statement as to its meaning had also been made by the ICRC—it is unlikely that delegates had a narrow understanding of the undertaking to ensure respect. They chose a broad formulation that accommodates an external scope, be it in terms of an entitlement or a duty.

Interestingly, the Commentaries to the Geneva Conventions published by the ICRC in the 1950s support the view that CA 1 imposes an obligation to ensure respect by others:

[In the event of a Power failing to fulfil its obligations, the other Contracting Parties (neutral, allied or enemy) may, and should, endeavour to bring it back to an attitude of respect for the Convention. The proper working of the system of protection provided by the Convention demands in fact that the Contracting Parties should not be content merely to apply its provisions themselves, but should do everything in their power to ensure that the humanitarian principles underlying the Conventions are applied universally.]\textsuperscript{37}

\textsuperscript{33} Ibid.
\textsuperscript{34} Ibid.
\textsuperscript{35} It is impossible to know in retrospect what the delegates had in mind at the time. The fact is that none of them contradicted the ICRC statement. In this sense, it might be interesting to remember that most scholars consider that silence can be used as supporting evidence for acquiescence. See 13 I. C. MacGibbon, “The Scope of Acquiescence in International Law”, British Yearbook of International Law, Vol. 31, No. 143, 1954, in particular pp. 146–147. See also G. Distefano, above note 16, p. 48: “La doctrine, par ailleurs, tend à attribuer au silence valeur probatoire aux fins interprétatives par voie de comportement ultérieur des parties”.
\textsuperscript{36} E. David, above note 30, para. 3.13.
\textsuperscript{37} J. Pictet, above note 12, p. 16. Note that the original French version of Pictet’s Commentaries is clearer when it comes to delineating the dichotomy between the entitlement to act (pouvoir) and the obligation to do so (devoir): “Ainsi encore, si une Puissance manque à ses obligations, les autres Parties contractantes … peuvent-elles – et doivent-elles – chercher à la ramener au respect de la Convention” (ibid., p. 21). The original French version of Pictet’s Commentaries is even stronger in the case of the Third Geneva Convention, since it only refers to a duty: “Ceci vaut pour le respect que chaque État
Finally, the system of protection underpinning the Geneva Conventions as a whole seems to run counter to the arguments of those who dispute the external element of the obligation in CA 1. As pointed out by Frédéric Siordet:

The monstrous character of certain violations of the Conventions committed [during the Second World War] where there had been no scrutiny led to a modification of the very idea of scrutiny. It was no longer merely a question of recognizing the legitimate right of a belligerent to see that the Conventions were applied, and to facilitate his doing so. For the private right of belligerents was substituted the general interest of humanity, which demanded scrutiny, no longer as a question of right, but of duty.\textsuperscript{38}

Siordet puts forward the existence of the Protecting Powers in Articles 10/10/10/11 of the Geneva Conventions as an example of a provision strengthening CA 1.\textsuperscript{39} He adds that the legal obligations imposed upon the parties to a conflict no longer seem sufficient by themselves, which is why the Geneva Conventions “seek … in addition to provide for scrutiny and cooperation from outside the Parties to the conflict”.\textsuperscript{40} Indeed, the need for supervision had already been discussed at the 1929 Diplomatic Conference, but it was only fully developed and made mandatory in the Geneva Conventions of 1949.\textsuperscript{41}

At any rate, the acceptance of an obligation to ensure respect by others for both international and non-international armed conflicts was expressly acknowledged after the adoption of the Geneva Conventions and is also what emanates from an analysis of the (more relevant) subsequent practice in the application of the treaty.\textsuperscript{42}

**Sixty years of State practice**

In the first years after the adoption of the Geneva Conventions, the idea of third-party responsibility did not arouse much interest among government officials or even among scholars. It was only in 1968, in Tehran, that the United Nations

\begin{itemize}
  \item In his concluding remarks regarding common Article 10/10/10/11, Siordet considers that the reason for imposing such an obligation upon third States is precisely to “strengthen[] Article 1”. *Ibid.*, p. 71.
  \item *Ibid.* Although Siordet focuses on the role of Protecting Powers, he makes the link between this new function and the existence of a legal obligation to ensure respect by others as enshrined in CA 1. Moreover, he broadly defines this obligation as one of due diligence—an issue that this article addresses in a later section. Siordet writes in *ibid.*, p. 44, that:

    The Protecting Power, on the other hand, whose action takes place in the territory of a foreign country, has only limited means at its disposal. Nevertheless the Conventions make it compulsory, within the limits of these means, for the Protecting Power to lend its services and to exercise its scrutiny in the application of the Conventions, in so far as it is itself a Party to the Conventions. The formal obligation of Article 1 “The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances” is as compulsory for it as for the Parties to the conflict.
\end{itemize}
(UN) International Conference on Human Rights, in the preamble to Resolution XXIII, reminded States party to the Geneva Conventions of their responsibility to “take steps to ensure respect of these humanitarian rules in all circumstances by other States, even if they are not themselves directly involved in an armed conflict.”\textsuperscript{43} Although the resolution was adopted by sixty-seven votes to none, with two abstentions, it is not absolutely clear whether the term “responsibility” referred to a legal obligation or something less.\textsuperscript{44} However, the vast array of subsequent practice supports the imperative nature of the duty to ensure respect for States that are not party to an armed conflict.

The International Court of Justice (ICJ) has, on various occasions, asserted the imperative nature of the obligation to ensure respect. In the Nicaragua case, the Court considered that even though the United States was not a party to the NIAC, it had an obligation to ensure respect for the Geneva Conventions in all circumstances.\textsuperscript{45} It further added that this obligation did “not derive only from the Conventions themselves, but from the general principles of humanitarian law”.\textsuperscript{46} In its advisory opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, the Court underscored that “every State party to [the Fourth Geneva Convention], whether or not it is a party to a specific conflict, is under an obligation to ensure that the requirements of the instruments in question are complied with”.\textsuperscript{47}

Together with the ICJ, both the Security Council and the General Assembly have issued a myriad of resolutions\textsuperscript{48} reaffirming the existence of a legal obligation for third States to ensure respect for IHL in conflicts to which they are not a party.\textsuperscript{49} For instance, the Security Council has called upon third States to ensure compliance


\textsuperscript{44} Kalshoven has expressed doubts on construing Resolution XXIII as an implicit acceptance of the legal obligation enshrined in CA 1. F. Kalshoven, above note 9, p. 43. Other authors do not hesitate to support the opposite view. See e.g. F. Azzam, above note 12, p. 62.

\textsuperscript{45} ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment (Merits), 27 June 1986, para. 220.

\textsuperscript{46} Ibid.

\textsuperscript{47} ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Wall Case), Advisory Opinion, 9 July 2004, para. 158. See also ICJ, Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, 19 December 2005, paras 211 and 345. In this case, the ICJ did not analyse the issue of third States’ responsibility. However, it did indeed consider that the undertaking to ensure respect for IHL constituted a legal obligation under international law.

\textsuperscript{48} Condorelli and Boisson de Chazournes consider that “common Article 1 has in the last ten years [1990–2000] almost become a basic norm of behaviour ... within the framework of the United Nations”: see L. Condorelli and L. Boisson de Chazournes, above note 4, pp. 76–78, for a more detailed study on UN practice. See also Toni Pfanner, “Various Mechanisms and Approaches for Implementing International Humanitarian Law and Protecting and Assisting War Victims”. International Review of
with IHL in Israel/Palestine, Bosnia and Herzegovina and Rwanda. Furthermore, in a report submitted to the Security Council by the Secretary-General, it was unambiguously affirmed that:

Under [the Fourth Geneva Convention], each Contracting State undertakes a series of unilateral engagements, vis-à-vis itself and at the same time vis-à-vis the others, of legal obligations to protect those civilians who are found in occupied territories following the outbreak of hostilities ... the Security Council should consider making a solemn appeal to all the High Contracting Parties to the Fourth Geneva Convention that have diplomatic relations with Israel, drawing their attention to their obligation under article 1 of the Convention to "... ensure respect for the present Convention in all circumstances" and urging them to use all the means at their disposal to persuade the Government of Israel to change its position as regards the applicability of the Convention.

A similar appeal was made in Resolution 45/69 of December 1990, entitled "The Uprising (Intifadah) of the Palestinian People". Therein, the General Assembly not only requested the Occupying Power to abide by the provisions of the Fourth Geneva Convention, but also called upon all States party to that Convention "to ensure respect for Israel ... for the Convention in all circumstances, in conformity with their obligation under article 1 thereof". The same body has approved other quasi-identical resolutions in the last two decades.

Within the framework of the United Nations, such appeals have also been issued by the Sub-Commission on Human Rights and the Commission on Human Rights, as well as its successor the Human Rights Council.

The participants in the Diplomatic Conference of Geneva of 1974–1977 also included the obligation to ensure respect in Article 1(1) of the First Additional Protocol to the Geneva Conventions of 1949 and, as pointed out by

---

54 UN GA Res. 45/69, UN Doc. A/RES/45/69, 6 December 1990, para. 3.
55 See e.g. UN GA Res. 60/105, UN Doc. A/RES/60/105, 8 December 2005, para. 3; UN GA Res. 62/107, UN Doc. A/RES/62/107, 17 December 2007, para. 3; UN GA Res. 63/96, UN Doc. A/RES/63/96, 5 December 2008, para. 3; UN GA Res. 68/81, UN Doc. A/RES/68/81, 16 December 2013, para. 3; and UN GA Res. 68/82, UN Doc. A/RES/68/82, 16 December 2013, para. 7.
56 See e.g. UN Sub-Commission on Human Rights, Res. 1990/12, 30 August 1990, para. 4; Res. 1991/6, 23 August 1991, para. 4; Res. 1992/10, 26 August 1992, para. 4; and Res. 1993/15, 20 August 1993, para. 4.
57 See e.g. UN Commission on Human Rights, Res. 2005/7, 14 April 2005, preamble and para. 5. This resolution "calls upon Member States to take the necessary measures that fulfil their obligations.
Levrat, they decided to do so “with full knowledge of the facts”. In 1993, the Final Declaration of the International Conference for the Protection of War Victims reiterated that the responsibility to respect and ensure respect encompassed the need to guarantee “the effectiveness of international humanitarian law and take resolute action, in accordance with that law, against States bearing responsibility for violations of international humanitarian law with a view to terminating such violations”. Two years later, in 1995, Resolution 1 of the 26th International Conference of the Red Cross and Red Crescent, which was adopted by consensus, reaffirmed that “every State must respect in all circumstances the relevant principles and norms of humanitarian law and ... must ensure respect for the Conventions and Protocols”, thus leaving no doubt as to the imperative nature of this obligation.

The ICRC has consistently and publicly emphasized this aspect of CA 1 and reminded States of their obligations thereunder. It has taken a number of steps, confidentially or publicly, individually or generally, to encourage States, including those not party to a conflict, to use their influence or offer their cooperation in order to ensure respect for IHL. When it is deemed necessary in the interest of the victims to appeal to the responsibility of all High Contracting Parties regarding a specific situation, the ICRC chooses from a range of possibilities at its disposal, among which is the quite exceptional measure of making a public appeal. Appeals to High Contracting Parties expressly referring to CA 1 were made by the ICRC, for example, in 1974 (Middle East), in 1979 (Rhodesia/Zimbabwe), in 1980 (Afghanistan), in 1983 and again in 1984 (Iran and Iraq), in 1992 (Bosnia-Herzegovina) and in 1995 (Rwanda). Moreover, in a series of regional expert seminars organized by the ICRC in 2003 as preparation for the 28th International Conference of the Red Cross and Red Crescent, participants confirmed that by virtue of CA 1 third States are bound not only by a negative legal obligation to neither encourage a party to an armed conflict to violate IHL nor to take action that would assist in such violations, but also by a positive obligation to take appropriate action – unilaterally or collectively – against parties to a conflict who are violating IHL.

It has often been said that, due to the intrinsically confidential nature of the diplomatic machinery involved, it is difficult to record practice of individual States


61 See also 30th International Conference of the Red Cross and Red Crescent, Resolution 3, 2007. para. 2.
illustrating this obligation to ensure respect by third parties. Scholars in the early 1990s, in particular, therefore voiced a word of caution as to whether governments felt themselves obliged to intervene when a party to an armed conflict violated IHL. However, such passiveness was deemed “hard to justify, or even to understand”, considering the undeniable external component of the rule. As of today, thanks to an ever-growing tendency that has been gaining momentum over the last two decades, it is doubtful that one can keep questioning the lack of State practice illustrating this duty. Interestingly, in this respect, the EU felt the need to adopt guidelines on promoting compliance with IHL. As indicated under the section on purpose, it is emphasized that the “[g]uidelines are in line with the commitment of the EU and its Member States to IHL, and aim to address compliance with IHL by third States, and, as appropriate, non-State actors operating in third States”. The guidelines also state means of action at the disposal of the EU in relation to third countries.

Other, more contextual State practice also illustrates a sense of positive duty. For instance, in 1980, the member States of the European Economic Community (ECC), predecessor of the European Union, issued a joint statement, known as the Venice Declaration, considering that Israeli settlements were illegal under international law. Through the Venice Declaration, the ECC “stress[ed] the need for Israel to put an end to the territorial occupation which it has maintained since the conflict of 1967”. Since then, numerous European institutions, such as the European Council, the European Commission and the Council of the

65 H.-P. Gasser, above note 64, p. 32.
66 Ibid.
68 In addition to the practice specifically referenced in this article, see the ICRC database on State practice for further examples, available at: www.icrc.org/customary-ihl/eng/docs/v2_rul_rule144. As can be seen, and contrary to what is sometimes asserted (see Birgit Kessler, “The Duty to ‘Ensure Respect’ under Common Article 1 of the Geneva Conventions: Its Implications on International and Non-International Armed Conflicts”, German Yearbook of International Law, Vol. 44, 2001, p. 509), States have also acted and invoked CA 1 in situations of NIAC – see infra the cases of Syria, Libya and Sudan.
71 See e.g. European Commission, EU-Israel: Implementation of the Interim Agreement in the Framework of
European Union, as well as many EU representatives, have repeatedly— and publicly— emphasized that the building of settlements anywhere in the Occupied Palestinian Territories, including East Jerusalem, is prohibited by IHL.

Continued violations of human rights and IHL in the Darfur region led the United States to put in place a series of economic sanctions against Sudan. In particular, the United States imposed a trade embargo against Sudan, prohibited the importation of goods and services of Sudanese origin, and put into effect “targeted sanctions against individuals and entities contributing to the conflict in the Darfur region.” At any rate, as it will be seen below, economic sanctions are but one of the means available to ensure respect by others.

On the occasion of the armed conflict in Libya in 2011, countries from all over the world condemned indiscriminate attacks causing death among the civilian population and urged the Libyan government to respect IHL; in February 2011 the European Union approved a package of sanctions against Libyan leaders, including an arms embargo and a travel ban.

The current armed conflict in Syria has also given rise to a variety of situations in which third States have endeavoured to ensure respect for IHL by the belligerents. In May 2012, following the killing of civilians in the Syrian city of Houla, almost a dozen countries from the Americas, Europe and Australia expelled all Syrian diplomats from their respective territories as a means of protest. The EU (in association with various candidate and non-EU States) has referred explicitly to CA 1 in its diplomatic démarches to put an end to the “terrible” IHL violations committed in Syria, such as the denial of humanitarian assistance, the attacks against humanitarian workers, the use of siege and starvation as a method of warfare, indiscriminate attacks causing death among the civilian population and the recruitment of children into the armed forces:

The lack of respect for international humanitarian law and human rights is appalling and concerns us all … Common article 1 of the Geneva Conventions clearly requires that all the contracting Parties, and I quote, “undertake to respect and to ensure respect” for the conventions “in all circumstances”. Thus, it is a collective obligation on all of us not only to respect but also to ensure that the parties to the conflict respect their

humanitarian obligations. We need to ensure actual enforcement of the obligations.\textsuperscript{78}

All in all, taking into consideration both the drafting history of CA 1 and the subsequent practice of States, international tribunals and intergovernmental organizations,\textsuperscript{79} States not party to an armed conflict have a legal obligation to ensure respect for the Geneva Conventions, and for applicable IHL more broadly,\textsuperscript{80} through taking positive steps. What needs to be elucidated are the exact nature and extent of this legal obligation.

\textbf{Nature of the obligation to ensure respect}

Article 48 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts provides that any State other than an injured State is entitled to invoke the responsibility of another State if the obligation in question is “owed to the international community as a whole” – this is indeed the case with the Geneva Conventions, which lay down legal obligations of an \textit{erga omnes} nature.\textsuperscript{81} That said, the obligation to ensure respect in its external dimension, imposed by CA 1, is distinct from the right of third States to act vis-à-vis the breach of \textit{


\textsuperscript{79} For a brief analysis on how resolutions, declarations and other normative instruments adopted by international organizations can be constitutive of the \textit{opinio juris} of IHL rules, see Theodor Meron, \textit{Human Rights and Humanitarian Norms as Customary Law}, Clarendon Press, Oxford, 1989.

\textsuperscript{80} ICJ, \textit{Nicaragua v. United States of America}, above note 45, para. 220.

\textsuperscript{81} See International Criminal Tribunal for the Former Yugoslavia (ICTY), \textit{The Prosecutor v. Zoran Kupreskic and Others}, Case No. IT-95-16-T, Judgment (Trial Chamber), 14 January 2000, para. 519:

As a consequence of their absolute character, these norms of international humanitarian law do not pose synallagmatic obligations, \textit{i.e.} obligations of a State vis-à-vis another State. Rather – as was stated by the International Court of Justice in the Barcelona Traction case (which specifically referred to obligations concerning fundamental human rights) – they lay down obligations towards the international community as a whole, with the consequence that each and every member of the international community has a “legal interest” in their observance and consequently a legal entitlement to demand respect for such obligations.

omnes obligations under public international law. As shown in previous sections—and as can be seen from a significant amount of verbal State practice as expressed in international organizations/fora and elsewhere—CA 1 goes beyond an entitlement for third States to take steps to ensure respect for IHL. It establishes not only a right to take action, but also an international legal obligation to do so. The words “ensure respect” imply an active duty and the term “undertake” suggests a genuine obligation, and this applies to all aspects of CA 1—both the internal and the external component. The Commentaries on the Geneva Conventions, when it comes to the imperative nature of the undertaking to ensure respect by others, assert that CA 1 is not a stylistic clause but a provision invested with imperative force. A similar reading regarding the binding nature of the word “undertake” is made by the Commentaries on AP I, as well as by the ICJ in the context of the Genocide Convention. Furthermore, this is also what can be deduced from the language of the international rulings, resolutions and statements analysed in the previous section. Thus, the question at this point is not so much whether CA 1 imposes a binding obligation, but rather what type of obligation lies beneath it.

A duty of diligent conduct

International obligations—as well as domestic ones—can be divided into two types. On the one hand, there are obligations of result, which imply that a State must attain a

82 In the Wall Case, the ICJ made a clear distinction between the existence of erga omnes obligations within the body of IHL and the obligation imposed upon third States by CA 1 to ensure respect in all circumstances. See ICJ, Wall Case, above note 47, paras 155–159. For an in-depth analysis of the legal regime of erga omnes obligations, as well as of the diverging features of other treaty-based obligations in whose performance all contracting parties are said to have a legal interest (also referred to as erga omnes partes or erga omnes contractantes obligations), see Christian J. Tams, Enforcing Obligations Erga Omnes in International Law, Cambridge University Press, Cambridge, 2010, pp. 117–157.

83 ICJ, Nicaragua v. United States of America, above note 45, para. 220.

84 J. Pictet, above note 12, p. 17.


Since para. 1 does not limit the obligations of the High Contracting Parties to territories involved in the conflict, the obligation to ensure respect for the Protocol falls also upon Parties not involved in the conflict. They have to use any lawful means at their disposal in their international relations to ensure that the High Contracting Parties involved respect the Protocol.


The ordinary meaning of the word “undertake” is to give a formal promise, to bind or engage oneself, to give a pledge or promise, to agree, to accept an obligation. It is a word regularly used in treaties setting out the obligations of the Contracting Parties … It is not merely hortatory or purposive. The undertaking is unqualified … and it is not to be read merely as an introduction to later express references to legislation, prosecution and extradition. Those features support the conclusion that Article I, in particular its
specific outcome. On the other hand, there exist obligations of means, also called obligations of due diligence, where States are only obliged to follow a certain conduct, regardless of whether they attain the desired result or not. In summary, “the obligation of result is an obligation to ‘succeed’, while the obligation of diligent conduct is an obligation to ‘make every effort’.” 88 Some authors have considered that High Contracting Parties might be held liable for failure to fulfil their CA 1 obligation until the desired result of ensuring respect for the Geneva Conventions in all circumstances is achieved. 89 However, this can hardly be the case. A State not party to a specific armed conflict cannot be said to be under an obligation to reach a particular outcome—for example, the cessation of all IHL violations by a belligerent—with regard to that conflict. On the contrary, third States can only be under an obligation to exercise due diligence in choosing appropriate measures to induce belligerents to comply with the law. This does not turn the duty to ensure respect into a vacuous norm, since States are under the obligation, depending on the influence they may exert, to take all possible steps, as well as any lawful means at their disposal, to safeguard respect for IHL rules by all other States. 90 If they fail to do so, they might incur international responsibility. In this sense, it should be highlighted that the intricateness of international relations, including the political dynamics to which a State might be subject, does not diminish the validity of this obligation. 91 In fact, the opposite is true: a State with close political, economic and/or military ties (for example, through equipping and training of armed forces or joint planning of operations) to one of the belligerents has a stronger obligation to ensure respect for IHL by its ally. 92 This is precisely the underlying logic of CA 1, as well as of other IHL rules in which close ties between two States lead to the reinforcement of their exiting obligations. 93

Further guidance for the purposes of CA 1 can be drawn from the ICJ in the case _Bosnia and Herzegovina v. Serbia and Montenegro_. Therein, the ICJ found that the legal obligation to prevent genocide enshrined in Article 1 of the Genocide Convention was also one of due diligence. With regard to the due diligence standard, it held that States are obliged to use “all means reasonably available to them” and that a State incurs responsibility only if it has “manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the

88 Ibid., p. 48.
89 See e.g. F. Azzam, above note 12, pp. 73–74.
91 F. Azzam, above note 12, p. 74.
92 H-P. Gasser, above note 64, p. 28.
 genocide”. The ICJ further added that due diligence can only be assessed in concreto. This is the case with any obligation of due diligence, including the duty to ensure respect for IHL by others. Thus, only a case-by-case analysis can reveal whether a State has actually violated CA 1. For that purpose, together with the capacity to influence the parties to the conflict, it is important to take into consideration the seriousness of the potential violation. For instance, a non-belligerent State C could hardly justify its passiveness vis-à-vis grave breaches of the Geneva Conventions committed by State A against State B, in particular if State C has a “special relationship” with State A. Such a special relationship is even more pronounced if third States provide support, directly or indirectly, to a party to an ongoing armed conflict.

Possible measures to ensure respect

As for the possible measures for ensuring compliance with IHL available to States not party to an armed conflict, these can be classified into three broad categories. First, measures aimed at exerting diplomatic pressure: these include, inter alia, protests lodged with the corresponding ambassador, public denunciations, pressure through intermediaries and/or referral to the International Fact Finding Commission – in

94 See ICJ, Bosnia and Herzegovina v. Serbia and Montenegro, above note 86, para. 430:

It is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide: the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide so far as possible. A State does not incur responsibility simply because the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of “due diligence", which calls for an assessment in concreto, is of critical importance. Various parameters operate when assessing whether a State has duly discharged the obligation concerned. The first, which varies greatly from one State to another, is clearly the capacity to influence.

95 Ibid.

96 See Robert P. Barnidge, “The Due Diligence Principle under International Law”, International Community Law Review, Vol. 8, 2006, p. 118: “While general principles can, and should, be sketched in the abstract, here, as elsewhere, the assessment under the due diligence rule is necessarily specific to particular facts and circumstances.”

97 T. Pfanner, above note 48, p. 305.

98 A. Devillard, above note 9, p. 101; B. Kessler, above note 68, p. 506, states: “The intensity of the treaties’ violations is another element that is important for obliging the States to take further steps to ‘ensure respect’ of the Conventions. This already follows from the ratio legis of the Geneva treaties.”

99 According to Kessler, this “special relationship” originates from different factors, such as “common history, common ethnic roots or even geographical proximity”. Ibid., p. 506. As seen above, Gasser focuses on military and economic influence. See H.-P. Gasser, above note 64, p. 28.

100 For a full analysis of this question, see Umesh Palwankar, “Measures Available to States for Fulfilling their Obligation to Ensure Respect for International Humanitarian Law”, International Review of the Red Cross, Vol. 33, No. 298, 1993, pp. 9–25. See also the possible actions that the EU has identified in its guidelines on the promotion of IHL. (European Union, above note 67): political dialogue, general public statements.
the event that both States have accepted its competence – or the International Criminal Court. Second, coercive measures taken by the State itself, such as measures of retribution: the above-mentioned expulsion of Syrian diplomats might fall under this category. Third are measures taken in cooperation with an international organization.\footnote{102}{See e.g. \textit{ibid.}, Art. 89.}

Of course, States are free to choose among the different measures at their disposal. Nevertheless, CA 1 should not be used to justify a so-called “droit d’ingérence humanitaire”.\footnote{103}{L. Condorelli and L. Boisson de Chazournes, above note 4, pp. 76–78. See also H.-P. Gasser, above note 64, p. 29: “The right to take action with a view to ensuring full respect for humanitarian law by belligerents does not include the right to derogate from the prohibition to use force against another State. This seems to be uncontroversial.”} In principle, permitted measures must be limited to “protest, criticism, rejections or even non-military reprisals”.\footnote{104}{B. Kessler, above note 68, p. 506.} Armed intervention may only be decided within the context of the UN, and in full respect of the UN Charter.\footnote{105}{L. Condorelli and L. Boisson de Chazournes, above note 4, pp. 76–78. See also ICRC, “The ICRC’s Position on ‘Humanitarian Intervention’”, \textit{International Review of the Red Cross}, Vol. 83, No. 842, 2001, pp. 530–531: The question of what measures are to be taken by the States and the United Nations in order to put an end to [breaches of IHL] is not dealt with by humanitarian law, but rather by the UN Charter (Chapters VII and VIII) … If armed intervention is decided upon, the Security Council can decide whether it is to be carried out by the UN forces or delegated to a State or regional security body. However, Article 53 of the Charter specifies that “no enforcement action shall be taken under regional arrangements or by regional agencies without the authorization of the Security Council”.} The rules on the resort to armed force (\textit{jus ad bellum}) govern the legality of any use of force, even if it is meant to end serious violations of IHL. The content of CA 1 is not part of \textit{jus ad bellum} and thus cannot serve as a legal basis for the use of force.

Failing to take measures will give rise to the international responsibility of the third State only when its conduct cannot be deemed diligent. What needs to be proved is the inconsistency between the State’s actual conduct and the conduct demanded by the “due diligence standard”.\footnote{106}{Needless to say, the burden of proof is higher than in the case of obligations of result, where it suffices to demonstrate that the outcome required by the norm has not been reached. An additional hurdle exists in the case of the obligation to ensure respect, since diplomatic \textit{démarches} are often conducted bilaterally and discretely. Be that as it may, holding third States accountable for their failure to ensure compliance with IHL is more than a conjectural speculation – supposing, that is, that they do not meet the adequate “due diligence standard”. It remains to be seen what elements compose that standard.} Needless to say, the burden of proof is higher than in the case of obligations of result, where it suffices to demonstrate that the outcome required by the norm has not been reached. An additional hurdle exists in the case of the obligation to ensure respect, since diplomatic \textit{démarches} are often conducted bilaterally and discretely. Be that as it may, holding third States accountable for their failure to ensure compliance with IHL is more than a conjectural speculation – supposing, that is, that they do not meet the adequate “due diligence standard”. It remains to be seen what elements compose that standard.

\textbf{Specific content of the obligation to ensure respect}

In the \textit{Nicaragua} case, the ICJ considered that, by virtue of the duty to ensure respect, the United States was “under an obligation not to encourage persons or groups
engaged in the conflict in Nicaragua to act in violation of the provisions of [common Article 3 to the Geneva Conventions]."\textsuperscript{107} Since then, it has often been repeated that CA 1, as well as the general principles of humanitarian law to which it gives expression, prohibits third States from encouraging the parties to a conflict to violate IHL. As pointed out by Meron, the well-grounded principles of good faith and \textit{pacta sunt servanda} impose upon States party to the Geneva Conventions not only a duty to abide by their own obligations, but also a duty not to encourage other parties to violate theirs.\textsuperscript{108} Furthermore, according to the general regime of State responsibility, third States are under the obligation not to knowingly aid or assist in the commission of IHL violations.\textsuperscript{109} They also must refrain from recognizing as lawful any situation created by a serious breach of peremptory norms of IHL.\textsuperscript{110} All of these obligations can be considered negative duties, and even if CA 1 did not exist, they would flow from other norms of international law.\textsuperscript{111} To give but one example, such negative duties could arise in multinational operations. High Contracting Parties would be prevented from carrying out joint operations with other States if there was an expectation that these States would act in violation of the Geneva Conventions or other relevant norms of IHL, unless they took active measures to ensure respect therewith. Such measures to ensure respect could include joint planning, training or mentoring programmes. This logic lies at the heart of UN Security Council Resolution 1906,\textsuperscript{112} which reiterated that

the support of MONUC [United Nations Organization Stabilization Mission in the DRC] to FARDC-led [Armed Forces of the DRC] military operations against foreign and Congolese armed groups is strictly conditioned on FARDC’s compliance with international humanitarian, human rights and refugee law and on an effective joint planning of these operations.\textsuperscript{113}

However, the fact that these negative duties emanate from public international law, together with the above-mentioned practice, as well as the fact that CA 1 uses the term “ensure” in the active voice, indicates that the scope of the obligation to ensure respect is “undoubtedly larger than simply ‘not encouraging’”,\textsuperscript{114} and also includes a series of positive obligations.

\textsuperscript{107} ICJ, \textit{Nicaragua v. United States of America}, above note 45, para. 220.
\textsuperscript{108} T. Meron, above note 79, p. 31.
\textsuperscript{110} \textit{Ibid.}, Art. 41(2). See also ICJ, \textit{Wall Case}, above note 47, paras 158–159, recalling also CA 1.
\textsuperscript{113} The same logic could apply with a view to stopping and preventing violations, as shown in the following
Stopping IHL violations

To start with, High Contracting Parties have a duty to exert their influence/take appropriate measures to put an end to ongoing IHL violations. This aspect of CA 1 is the basis for Rule 144 identified in the ICRC Customary Law Study, which provides, *inter alia*, that States “must exert their influence, to the degree possible, to stop violations of international humanitarian law”.115

The above-mentioned abstract from the Commentaries to the Geneva Conventions already established that in the event of a belligerent failing to fulfil its obligations, third States have an obligation to “endeavour to bring it back to an attitude of respect for the Convention”.116 *Prima facie*, the idea of bringing back one of the parties to the conflict to an attitude of respect implies that a violation of IHL has previously taken place. The Commentary to the First Additional Protocol equally echoed this aspect of the obligation.117 According to expert participants in the five seminars organized by the ICRC in 2003 on the issue of improving compliance with IHL, States not involved in an armed conflict have a positive obligation to “take action … against States who are violating international humanitarian law, in particular to intervene with States over which they might have some influence to stop the violations”.118

Such an obligation to stop IHL violations is evidenced specifically in Article 89 of AP I, which provides that “[i]n situations of serious violations of the Conventions or of this Protocol, the High Contracting Parties undertake to act jointly or individually, in cooperation with the United Nations and in conformity with the United Nations Charter”.

Many of the examples of State practice mentioned above were actually aimed at putting an end to situations that contravened basic humanitarian norms and, as shown by the ICRC Customary Law Study, they account for a well-grounded legal obligation. But going one step further, it is worthwhile pondering whether, in addition to requiring third States to exert their influence/take appropriate measures to bring ongoing violations to an end, the duty to ensure respect in its external dimension also includes a preventive component.

Preventing IHL violations

If one looks at CA 1 against the backdrop of the atrocities committed during the Second World War, and in the light of its object and purpose, there are strong arguments that support an undertaking to prevent violations of the Conventions. An illustration of the eagerness of States at the time of negotiating the Geneva Conventions to avoid falling back into the scourges of the Second World War is manifest in Article 1 of the Genocide Convention, adopted only a few months


116
earlier than the Geneva Conventions. In that Article, the “Contracting Parties confirm that genocide, whether committed in time of peace or in time of war, is a crime under international law which they undertake to prevent and to punish”. Looking at that provision, the ICJ held that the word “undertake”—the same used by CA 1—sets a legally binding obligation,\(^{119}\) and asserted that the obligation of States was one of conduct, which could be breached if they failed to take all measures within their power to prevent genocide.\(^{120}\) Interestingly, the ICJ further added that claiming, or even proving, that the means reasonably at the disposal of a State were insufficient was irrelevant for the purposes of breaching the obligation, since “the combined efforts of several States, each complying with its obligation to prevent, might have achieved the result—averting the commission of genocide—which the efforts of only one State were insufficient to produce”.\(^{121}\) It is submitted that this whole framework is indeed similar to the one underpinning CA 1, and which Pilloud described as an obligation for all High Contracting Parties to “do all in their power to see that the basic humanitarian principles of the Conventions were universally applied”.\(^{122}\)

Several scholars have posited that the obligation to ensure respect includes a duty to take measures to prevent IHL violations. For instance, Devillard argues that although reacting to illicit conduct—that is, stopping ongoing breaches of a rule—constitutes the “heart” of CA 1, the role of prevention should not be neglected.\(^{123}\) He adds that the consequences of IHL violations are often too serious to simply accept “a posteriori interventions”.\(^{124}\) Although, according to Devillard, a general obligation of prevention incumbent on third States can be excluded, an obligation to prevent IHL violations would be triggered in situations where the risk of such violations can be reasonably foreseen.\(^{125}\) In his analysis of the *erga omnes* obligation to ensure respect by others, Gasser refers not only to stopping violations, but also to “prevent[ing] further breaches from happening” and “act[ing] when parties to an armed conflict are likely to disregard the law or are about to violate their humanitarian obligations”.\(^{126}\) Other authors seem to go even further when they frame CA 1 primarily as a duty to “avert the occurrence of violations”, instead of only acting at the stage at which the misbehaviour has already taken place.\(^{127}\) It is not possible in abstract to elucidate the criteria under which non-belligerent States could incur international responsibility for their failure to prevent the violation of IHL rules. At any rate, it is clear that this obligation, being one of due diligence, only arises in cases in which the prospective


\(^{120}\) *Ibid.*, para. 430.

\(^{121}\) *Ibid.*

\(^{122}\) Final Record of the Diplomatic Conference of Geneva of 1949, above note 5, p. 53.

\(^{123}\) A. Devillard, above note 9, p. 96.

\(^{124}\) *Ibid.*

\(^{125}\) *Ibid.*, pp. 96 (where Devillard speaks of a specific risk) and 97 (“une obligation de prévention des violations des violations de IHL”).
inobservance of IHL is marked by a certain degree of predictability. That is why Gasser resorts to the idea of likelihood and Devillard to foreseeable risk. Indeed, under international law, due diligence obligations involving the need to prevent a particular event can only be triggered if the event in question is actually foreseeable.\(^\text{128}\)

The High Contracting Parties themselves have also endorsed this interpretation of CA 1 during the 30th International Conference of the Red Cross and Red Crescent, where they stressed

the obligation of all States to refrain from encouraging violations of international humanitarian law by any party to an armed conflict and to exert their influence, to the degree possible, to prevent and end violations, either individually or through multilateral mechanisms, in accordance with international law.\(^\text{129}\)

Moreover, UN pronouncements also point in this direction. For instance, a Security Council resolution from 1990 dealing \textit{inter alia} with the intention of the government of Israel “to resume”\(^\text{130}\) the deportation of Palestinian civilians in the occupied territories—that is, a potential IHL violation which had not yet occurred—called upon “the High Contracting Parties to [the Fourth Geneva Convention of 1949] to ensure respect by Israel, the occupying Power, for its obligations under the Convention in accordance with Article 1 thereof”.\(^\text{131}\) In such instances, the obligation to ensure respect should clearly be seen through the prism of prevention.

As a matter of fact, the duty to ensure respect by others has been conceived of as a general principle informing the entire field of IHL implementation.\(^\text{132}\) In this sense, it is interesting to note that measures to enforce IHL usually revolve around the concepts of repression and prevention,\(^\text{133}\) and that in fact, according to Marco Sassòli, the focus between these two elements must always be placed on the latter.\(^\text{134}\)


In general, in the context of prevention, a State of origin does not bear the risk of unforeseeable consequences ... [D]ue diligence is manifested in reasonable efforts by a State to inform itself of factual and legal components that relate foreseeably to a contemplated procedure and to take appropriate measures, in timely fashion, to address them. Thus, States are under an obligation to take unilateral measures to prevent significant transboundary harm or at any event to minimize the risk thereof.

Note that “the ILC’s description of the due diligence principle can be analogized to international law generally when the operative rule at issue imposes a due diligence obligation” (R. P. Barnidge, above note 96, p. 117).

\(^{129}\) 30th International Conference of the Red Cross and Red Crescent, Resolution 3, 2007, para. 2.

\(^{130}\) UN SC Res. 681, above note 50, para. 3.

\(^{131}\) \textit{Ibid.}, para. 5.

\(^{132}\) A. Devillard, above note 9, p. 113.

\(^{133}\) T. Pfanner, above note 48, p. 280.
Thus, considering this preventive component as part of the duty to ensure respect would be coherent not only with the means whereby IHL is usually implemented, but also with the manner in which CA 1 itself has often been framed.

All in all, and despite the need for further State practice and academic research elucidating the scope of this international legal obligation, it seems that prevention is inextricably intertwined with the duty to ensure respect. Failing to acknowledge this preventive aspect would probably be inconsistent with the raison d'etre of the Conventions, one of their main goals being to forestall the transgression of their rules. In fact, CA 1 is only one of the mechanisms envisioned by the drafters of the Geneva Convention to attain this objective. Other examples include:

1. The supervisory role of the Protecting Powers.
2. The obligation to disseminate the content of the Geneva Conventions as widely as possible, “in time of peace as in time of war”.
3. The obligation to enact legislation to provide effective penal sanctions for and to repress grave breaches of the Geneva Conventions and AP I.
4. The obligation to “take measures necessary for the suppression of all acts contrary to the provisions of the present Convention other than ... grave breaches”. According to the Commentaries, the latter implies that States must do all they can to prevent the commission or repetition of acts contrary to the Conventions.

Moreover, part of the reason why States must bring ongoing IHL abuses to an end – in conformity with CA 1 – is also to prevent them from occurring again in the future.

Hence, it seems that CA 1 can and must be raised on its own whenever it helps to safeguard respect for the Geneva Conventions, and arguably for the whole body of

135 See e.g. Y. Sandoz, above note 111, p. 299: “Il nous a paru que l’on pouvait distinguer trois types de moyens [pour la mise en œuvre du droit international humanitaire]: le moyens préventifs ... les moyens de contrôle ... [et] les moyens de répression.”
136 B. Kessler, above note 68, p. 499, with further references:

Article 1 does not state anything about how the States shall ensure that the Conventions are respected ... Under the assumption that “ensuring respect” of a rule means making someone respect it, there are four means of enforcement: (1) repressive action against any violation of the Conventions, (2) help by one State to enable another State to fulfil its duties under the Conventions, (3) control, and (4) prevention.

137 Geneva Conventions, Arts 10/10/10/11.
139 Geneva Conventions, Arts 49/50/129/146; AP I, Arts 11, 85 and 86.
140 Geneva Conventions, Arts 49(3)/50(3)/129(3)/146(3).
141 Jean Pictet (ed.), Commentary: I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1952, p. 367: “The expression ‘faire cesser’, employed in the French text, is open to various interpretations. In our opinion it covers everything a State can do to prevent the
IHL, including when it comes to the obligation to prevent violations of its rules. A very clear example thereof can be found in the context of the Arms Trade Treaty (ATT). 143

The ATT and the obligation ensure respect

Modern efforts to control the humanitarian consequences of the arms trade can be traced back to the Brussels Conference Act of 1890. Therein, approximately twenty nations prohibited the introduction of firearms and ammunition to the Congo basin, with a view to curbing their “pernicious and prevailing role” in the slave trade and wars in Africa. 144 Since then, international law has struggled to find an adequate balance between the legality of arms and the need to rein in some of their more deleterious effects. This debate has been gaining momentum in the last fifteen years, culminating with the recent adoption of the ATT.

In 1998, over twenty like-minded States gathered in Oslo for the first time to specifically discuss the challenges raised by the spread of small arms. 145 They drew up a document wherein they recognized the humanitarian and security concerns linked to the arms trade and enumerated a series of existing norms that needed to be developed in order to address the problem. In particular, they referred to the obligation to respect and ensure respect for IHL. 146 A year later, in a study entitled Arms Availability and the Situation of Civilians in Armed Conflict, the ICRC, concerned about “the proliferation of weapons in the hands of new and often undisciplined actors”, 147 recommended that States “review their policies concerning the production, availability and transfer of arms and ammunition” in light of their responsibility under CA 1. 148 Since then, numerous codes of conduct on arms exports have incorporated compliance with IHL as part of their criteria for authorizing transfers. For instance, the Organization for Security and Cooperation (OSCE) Document on Small Arms and Light Weapons requires participating States to avoid issuing licenses for exports where they deem that there is a “clear risk” that the arms in question might “threaten compliance with international law governing the conduct of armed conflict”. 149 Instruments laying down similar criteria include the Organization of American States (OAS) Model Regulations for the Control of Brokers of Firearms, 150 the Economic Community of West African States (ECOWAS) Convention on Small Arms and

144 General Act of the Brussels Conference Relative to the African Slave Trade, Brussels, 2 July 1890, Art. VIII.
149 308th Plenary Meeting of the OSCE, Document on Small Arms and Light Weapons, FSC.DOC/1/00/Rev.1, 24 November 2004, Section III(A)(2)(b)(v).
Light Weapons\textsuperscript{151} and the Best Practice Guidelines for the Implementation of the Nairobi Declaration.\textsuperscript{152} All of these conventions and guidelines tend to focus on the likelihood of prospective IHL violations in order to establish whether weapons can be legitimately transferred. Thus, their main focus is to “avert the occurrence” of such abuses in the future— that is, to prevent them. \textsuperscript{153}

During the 28th International Conference of the Red Cross and Red Crescent, the High Contracting Parties to the Geneva Conventions endorsed a similar interpretation of the role played by CA 1 vis-à-vis the prevention of IHL violations in this domain:

In recognition of States’ obligation to respect and ensure respect for international humanitarian law, controls on the availability of weapons are strengthened—in particular on small arms, light weapons and their ammunition— so that weapons do not end up in the hands of those who may be expected to use them to violate international humanitarian law.\textsuperscript{154}

The UN General Assembly gave further impulse to these efforts by adopting Resolution 61/89 of 2006, where it requested the creation of a group of experts to examine the “feasibility, scope and draft parameters for a comprehensive, legally binding instrument establishing common international standards for the import, export and transfer of conventional arms”.\textsuperscript{155} However, even at that time, it was clear that—from an IHL perspective—if the ATT negotiations succeeded, the new legal instrument would only complement the already existing obligation to ensure respect by others.\textsuperscript{156} That is precisely the reason why a solid majority of States supported from the outset the view that respect for IHL should become one of the main criteria in the assessment of arms transfers within the treaty.\textsuperscript{157} As a

\textsuperscript{151} Ecowas, Convention on Small Arms and Light Weapons, Their Ammunition and Other Related Materials, 2006, Art. 6(2): “A transfer shall not be authorised if its authorisation violates obligations of the requesting States, as well as those of Member States, under international law, including ... universally accepted principles of international humanitarian law.”

\textsuperscript{152} Regional Centre on Small Arms and Light Weapons, Best Practice Guidelines for the Implementation of the Nairobi Declaration and the Nairobi Protocol on Small Arms and Light Weapons, 2005, p. 25:

State Parties shall not authorize transfers which are likely to be used ... (ii) for the commission of serious violations of international humanitarian law; (iii) in acts of aggression against another State or population, threatening the national security or territorial integrity of another State, or threatening compliance with international law governing the conduct of armed conflict.

\textsuperscript{153} N. Levrat, above note 59, p. 277.

\textsuperscript{154} 28th International Conference of the Red Cross and Red Crescent, Agenda for Humanitarian Action, Geneva, 2003, final goal 2(3). In a report submitted to High Contracting Parties during the 31st International Conference of the Red Cross and Red Crescent, the ICRC reiterated that the obligation to ensure respect “entails a responsibility [for all States] to make every effort to ensure that the arms and ammunition they transfer do not end up in the hands of persons who are likely to use them in violation of IHL”: ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflict, report of the 31st International Conference of the Red Cross and Red Crescent, October 2011, p. 46.
matter of fact, evaluating the level of respect for IHL before authorizing the export of arms has been considered an international legal obligation of a customary nature.\textsuperscript{158}

The ATT was adopted by the UN General Assembly in April 2013.\textsuperscript{159} It included a very explicit reference to CA 1. Indeed, the duty to “[r]espect[] and en[sure][e] respect for international humanitarian law in accordance with, \textit{inter alia}, the Geneva Conventions of 1949” was deemed one of the fundamental principles pervading the whole document.\textsuperscript{160} Against the backdrop of this principle, Article 6(3) of the ATT established that a State Party must not authorize any transfers of conventional arms if it has knowledge that the weapons would be used in the commission of grave breaches to the Geneva Conventions of 1949, attacks against civilians or civilian objects, or other war crimes as defined by international agreements to which it is a party. Even if the export is not prohibited under Article 6, the following Article prohibits transfer if there is an “overriding risk” that the weapons might be used to commit or facilitate a serious violation of IHL.\textsuperscript{161} As for the criteria States may use to assess the risk of transferring arms or military equipment, the ICRC has proposed a variety of indicators that include the recipient’s past and present IHL record, the recipient’s alleged intentions—as expressed through its own commitments—and the recipient’s capacity to ensure that the weapons in question are not used in a manner that is inconsistent with IHL.\textsuperscript{162}

It should be noted that, as previously seen, the obligation to ensure respect cannot be circumscribed to the mere prohibition of aiding or assisting in the commission of IHL violations.\textsuperscript{163} Therefore, in the context of arms transfers, CA 1 also prescribes a series of positive obligations that go beyond the wording of Article 16 of the Draft Articles on Responsibility of States. According to the International Law Commission, aid or assistance are only unlawful when the assisting State has knowledge of the circumstances that make the conduct illegal and decides to carry out such conduct with a view to facilitating the violation. In the case of arms exports, Draft Article 16 can be translated in the following manner: State C would only incur international responsibility if it sells weapons to State A in order to facilitate the infringement of IHL against State B, and with knowledge that the weapons will be used for such purpose. In contrast, CA 1 would require State C to assess whether State A is likely to use the weapons to violate IHL in an armed conflict with State B, and to refrain from transferring the arms if there is a substantial or clear risk that they could be used in that manner.\textsuperscript{164}

\textsuperscript{160} \textit{Ibid.}, 5th principle of the preamble.
\textsuperscript{161} \textit{Ibid.}, Arts 7(1)(b)(i) and 7(3).
\textsuperscript{163} M. Sassoli, above note 134, n. 413
At any rate, the legal debate that led to the adoption of the ATT is but one example of the ways in which CA 1 can contribute to endeavours to improve compliance with IHL. There can be no doubt as to the great potential of the duty to ensure respect by others when it comes to enforcing IHL rules in other domains—for instance, by clarifying the obligation of multinational forces during the transfer of detainees. 165

**Conclusion**

CA 1 epitomizes the commitment of States to avoid IHL violations taking place in the future. It does so by creating a framework whereby States not party to a particular armed conflict must use every means at their disposal to ensure that the belligerents comply with the Geneva Conventions and AP I, and probably with the whole body of IHL. 166 As shown by this article, CA 1 is not a mere entitlement to act. Instead, it imposes upon third States an international legal obligation to ensure respect in all circumstances. This obligation, which applies in international and non-international armed conflicts, is one of due diligence: to avoid breaching it, States must make every lawful effort in their power, regardless of whether they attain the desired result or not. For that purpose, they can choose among the different means at their disposal—with the exception of military intervention, which would only be lawful if undertaken in accordance with the UN Charter. That said, as in many other branches of international law, the larger the means, the greater the responsibility.

With regard to the content of the obligation to ensure respect in its external dimension, CA 1 clearly includes a duty of third States not to encourage persons or groups engaged in an armed conflict to act in violation of the Geneva Conventions, nor to knowingly aid or assist in the commission of such violations. Nonetheless, CA 1 goes well beyond this negative duty. Firstly, it includes an obligation to put an end to ongoing IHL violations. Secondly, the obligation to ensure respect encompasses the duty to prevent breaches of IHL from occurring.

In a world where compliance with existing rules seems to be the main hurdle to limiting the effects of armed conflict and to adequately protecting

---

165 See e.g. Cordula Droge, “Transfer of Detainees: Legal Framework, Non-Refoulement and Contemporary Challenges”, *International Review of the Red Cross*, Vol. 90, No. 871, 2008, p. 687. Droeg makes the link between the transfer of detainees and the obligation to ensure respect, which—as already indicated—also applies to multinational forces:

Beyond the responsibility arising from direct attribution to them, international organizations are also bound by the obligation to ensure respect for international humanitarian law. Thus, if a multinational operation is carried out under the umbrella of an international organization, that organization is particularly well placed to take steps to prevent and terminate violations of international humanitarian law committed by the State. In such cases it should exert its influence as far as possible
persons who are not or are no longer participating in hostilities, underscoring the preventive component of the legal obligation established by CA 1 is of paramount importance. Third States, thanks to their more neutral stance vis-à-vis the dynamics of the conflict, are in a privileged position to ensure that the "general principles of humanitarian law to which the Conventions merely give specific expression"\textsuperscript{167} are respected universally. It can only be hoped that they will live up to the commitment they made when they subscribed to a body of law whose main purpose is precisely to prevent violations of the very same rules it enunciates.
Ensuring Responsibility: Common Article 1
and State Responsibility for Non-State Actors

Oona A. Hathaway, Emily Chertoff, Lara Domínguez,
Zachary Manfredi and Peter Tzeng*

In Syria, the United States is “training and equipping” non-state groups to battle ISIS. In Eastern Ukraine, Russia has provided weapons, training, and support to separatists. In China, “private” computer hackers create codes designed to infiltrate sensitive computer systems. These are just a few examples of the many ways in which states work with non-state actors to accomplish their military and political objectives. While state/non-state collaboration can be benign, it can be malignant where a state uses a non-state actor as a proxy to violate international law with impunity. In extreme

*Gerard C. and Bernice Latrobe Smith Professor of International Law, Yale Law School; J.D. candidate, Yale Law School (expected 2017); J.D. candidate, Yale Law School (expected 2016); J.D. candidate, Yale Law School (expected 2017), Ph.D. candidate in Rhetoric, UC Berkeley (expected 2018); J.D. candidate, Yale Law School (expected 2016), respectively. We are grateful to participants in the ICRC and Cardozo Law School workshop on “Revisiting the Role of International Law in National Security,” especially Beth Van Schaack. We also thank Rebecca Crotofo, Daniel Hessel, Julia Shu, and Sarah Weiner for their input from the beginning of this project. All remaining errors are our own.
cases, a state could go as far as to fund, train, and instruct a non-state actor to commit war crimes and escape without international legal responsibility. This is no mere academic hypothetical: consider the Former Republic of Yugoslavia’s support of the Free Serbian Army, which committed the genocide at Srebrenica.

Recognizing this problem, international courts have developed a doctrine of state responsibility designed to hold states accountable for internationally wrongful acts of their non-state actor partners. Unfortunately, existing doctrine leaves an accountability gap and fails to correct the perverse incentive to use non-state actors as proxies for illegal acts. Moreover, it creates a second perverse incentive: states with good intentions might avoid training non-state actors in international law compliance to avoid crossing the “bright line” for attribution.

This Article proposes a fix to these problems, drawing on a novel interpretation of the Geneva Conventions released by the International Committee of the Red Cross (ICRC) in March 2016. It argues that the duty “to ensure respect” in Common Article 1 can fill the gap. In addition, it argues that Common Article 1 will be more widely embraced, and therefore more effective, if states that have exercised due diligence to prevent violations are allowed an affirmative defense against liability for any ultra vires violations. The Article concludes with recommendations for states that wish to fulfill their Common Article 1 obligations in good faith while
working with non-state actors.

[TOC will be reinserted]

Introduction

States frequently work with and through non-state actors, sometimes in cases where direct state action would have been politically or legally suspect. During the past few years, for example, the United States has financed, armed, and trained opposition forces in Syria.¹ Russia has assisted and supplied separatist forces in eastern Ukraine.² Iran continues to arm and fund Hezbollah in Lebanon.³ Across the globe, states continue to work with and through non-state actors engaged in armed conflict.⁴ Moreover, in many of

---


⁴ The question of state responsibility for non-state-actor conduct certainly exceeds the context
these cases, non-state actors take actions that would violate international law if undertaken directly by a state or its organs.5

of armed conflict. Our inquiry here, however, focuses primarily on attempting to resolve the accountability gap in the armed conflict context. We focus our attention here for at least three reasons: first, while it is ambiguous what aspects of international law apply to non-state actors generally, in the armed conflict context it is clear that non-state groups, at a minimum, have obligations under Common Article 3 of the Geneva Conventions; second, the control tests for attribution of state responsibility themselves have been developed through assessment of non-state actors' roles in armed conflict; third, our proposed solution to the accountability gap relies on international obligations that apply in the context of armed conflict. We do not claim that the solution we offer here would suffice to close the accountability gap for all state engagement with non-state actors, but nevertheless hope that it may gesture toward future avenues of research for closing the gap entirely.

5. There is substantial literature dealing with the issue of what law binds non-state actors in the context of armed conflict. While norms in this area are continuing to develop, for the purposes of this essay we assume the consensus that Common Article 3 of the Geneva Conventions applies to organized non-state groups that are party to an armed conflict. See Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 3, Aug. 12, 1949, 6 U.S.T. 3516, 3518–20. Additionally, while not weighing in here into the complex debates about the scope of international law obligations that regulate non-state actors, we nevertheless argue that, at a minimum, it is quite clear that international law obligates state conduct in the context of armed conflict more extensively than it does the conduct of non-state actors. See Christian Henderson, Non-State Actors and the Use of Force, in NON-STATE ACTORS IN INTERNATIONAL LAW 77–111 (Math Noortmann, August Reinisch & Cedric Ryngaert eds., 2015) (arguing that international law governing the use of force does not necessarily regulate the activities of non-state actors, such as terrorist groups, especially not to the extent such rules and norms govern the response of states that fall victim to terrorism); Andrew Clapham, Human Rights Obligations for Non-State-Actors: Where are We Now?, in DOING
This raises a pressing issue: When is a state responsible for the actions of a non-state actor? This question leads, in turn, to a host of additional questions: What degree of control does a state need to exercise over a non-state actor to be held liable for that actor's conduct? What actions should states take to ensure their non-state partners comply with their international law obligations? When states train and advise groups not to commit violations of international law, should they be held responsible when those actors do commit violations?

This problem is not new. The use of non-state actors as proxies was a prominent feature of the Cold War, perhaps most famously in the Bay of Pigs Invasion in 1961 and the proxy war in Afghanistan throughout the 1980s.

---


But the problem has risen to new prominence in recent years. Faced by stringent legal limits on their own direct action, states have exploited what has become a large and growing loophole in the international legal framework: States that work through non-state actors operate in a zone of legal uncertainty. As long as the doctrine of state responsibility for the actions of non-state actors remains unclear, states can exploit that uncertainty to make an end-run around their own legal obligations. This allows states to appear to abide by the law, while achieving all their illegal aims indirectly through non-state actors that would be unable to act without their support. The potential damage to the international legal framework is enormous.

In this Article, we argue that existing state-responsibility doctrine is insufficient to meet the current challenges. The International Law Commission’s Draft Articles on state responsibility and the jurisprudence of the international courts have continued to rely on a variety of “control tests” to determine the scope of state responsibility for non-state actor conduct. The current law of state responsibility focuses on whether the actions of a non-state actor can be “attributed” to a state. Under the framework for attribution, states must be shown to exercise a sufficient degree of control over the act or the actor in order to be held liable for non-state actors’

---

8. See infra note 13 and accompanying text.
commission of internationally wrongful acts. Yet despite states’ pervasive engagement with non-state actors, courts have rarely found states liable under these control tests. The resulting framework has led to a critical accountability gap in state responsibility doctrine: States too often effectively escape responsibility for violations of the laws of armed conflict if they act through non-state partners. It has also created dangerous incentives for states. They not only have little reason to police the actions of non-state actors that fall below the threshold for attribution, they may even be actively discouraged from taking actions to mitigate the danger of international humanitarian law violations by non-state actors: They may worry that taking measures to prevent violations could cause them to exercise control that might subject them to liability even for ultra vires acts.

In March 2016, the International Committee of the Red Cross (ICRC) issued new Commentaries on the Geneva Convention—the first in more than six decades.9 Contained within them is a possible answer to the problem created by modern state-responsibility doctrine: Common Article 1 of the Geneva Conventions obligates states to “undertake to respect and to ensure

---

9. The ICRC released a new set of commentaries in March 2016. This was the most extensive ICRC commentary since the Pictet commentaries, which were released in four volumes between 1952 and 1959. See JEAN PICTET, COMMENTARY ON THE GENEVA CONVENTIONS OF 12 AUGUST 1949 (1952-1959).
respect" for the Conventions in all circumstances.\textsuperscript{10} The ICRC commentaries\textsuperscript{11} conclude that Common Article 1 imposes not only negative obligations on states not to encourage violations of the law of armed conflict, but also positive third-party obligations on a state that closely coordinates its activities with non-state actors.\textsuperscript{12}

\begin{itemize}
\item \textsuperscript{11} ICRC, Commentary of 2016, art. 1 ¶ 154 (2016) ("This duty to ensure respect by others comprises both a negative and a positive obligation. Under the negative obligation, High Contracting Parties may neither encourage, nor aid or assist in violations of the Conventions by Parties to a conflict. Under the positive obligation, they must do everything reasonably in their power to prevent and bring such violations to an end.").
\item \textsuperscript{12} It is also important to note that Common Article 1 places affirmative responsibilities on states in both a non-international armed conflict (a conflict between a state and one or more non-state actors), and an international armed conflict (where two or more states are parties). \textit{Id.} art. 1, ¶ 125 ("The High Contracting Parties undertake to respect and to ensure respect for ‘the present Convention’ in all circumstances. ... Thus, the High Contracting Parties must also ensure respect
\end{itemize}
The precise scope of Common Article 1 obligations—in particular, whether Common Article 1 places any affirmative responsibility on states to ensure respect by actors it does not work with directly—has yet to be clarified by the ICRC. Nonetheless, this little-noticed provision carries immense possibility: It could close much of the gap in state responsibility for non-state actors in armed conflict situations. Some states might worry that Common Article 1 places them in a no-win situation: If they do not take steps to meet positive Common Article 1 obligations, they are in violation of their Geneva Convention obligations. But if they do take actions necessary to meet positive Common Article 1 obligations, they may end up exercising sufficient “control” to trigger state responsibility—even for *ultra vires* actions. Indeed, it is precisely this danger that may be leading some states to resist the broader interpretation of Common Article 1 advocated by the ICRC. To address this concern, we propose an affirmative defense for actions taken by states in furtherance of their Common Article 1 duties. Doing so would be consistent with the intent of the applicable legal framework and would create the right incentives for state and non-state actor compliance with the laws of armed conflict. States would be obligated to ensure their non-state partners abide by their international humanitarian law obligations, without worrying that

for the rules applicable in non-international armed conflict, including by non-State armed groups.

While not all of the Articles of the Geneva Convention apply in an armed conflict, the “duty to ensure respect” that this Article discusses does.
actions taken to assure such compliance would increase the state’s risk of liability for the non-state groups’ ultra vires actions.

The remainder of this Article is organized into five sections. Part I offers an overview of the current framework for attribution and the problems associated with the high evidentiary burdens that exist under its control tests for state responsibility. This Part aims not only to provide background for the argument that follows, but also to bring clarity to an important body of law that is frequently misunderstood. Part II provides an analysis of the perverse incentives that the modern attribution framework creates for state actors that wish to collaborate with non-state actors in the context of armed conflict. Part III examines state obligations under Common Article 1 of the Geneva Conventions and shows how the ICRC’s new proposed positive “due diligence” standard could ameliorate the gap in state responsibility doctrine. Part IV proposes a new affirmative defense for actions taken in furtherance of compliance with Common Article 1 duties. Finally, Part V offers a set of ex ante and ex post recommendations to states seeking to fulfill their obligations to ensure non-state partners comply with international law in the context of armed conflict.

I. The Current Legal Framework

The International Law Commission (ILC), International Court of Justice (ICJ), and International Criminal Tribunal for Yugoslavia (ICTY) have all considered the problem of state responsibility for the actions of non-state
actors in the context of armed conflict. Though these efforts have addressed elements of the accountability gap for the actions of non-state actors, they have thus far failed to resolve the problem.

There are several reasons for this failure. The first, and most obvious, is that each has taken a different—and sometimes even contradictory—approach to the dilemma of state responsibility. This has led to widespread confusion among those seeking to make sense of the legal obligations on states. Even putting the confusion and contradiction to one side, each of the approaches to the doctrine of state responsibility shares an additional, more troubling, shortcoming: Each treats state responsibility as a bright line test—a state is responsible, or it is not. There is nothing in between. This is because the doctrine of state responsibility has been centered around the question of attribution: Is the conduct of this non-state actor attributable to a state? In other words, should the conduct of the non-state actor be treated as if the state itself were the actor?

As we shall show in the sections that follow, this approach to state responsibility is at once too lenient and too strict. On the one hand, until a state passes the bright line and triggers state responsibility, it will not be held accountable for the actions of non-state actors. This is true even if the state has enabled a non-state actor to engage in behavior that violates international law and even if the state provided the enabling support with the intention that the non-state actor take actions that the state is itself legally prohibited from
taking (for instance, an illegal use of force or extrajudicial killing). On the other hand, the bright-line approach to state responsibility also means that once states cross over the line for triggering state responsibility, they may be held responsible for the actions of non-state actors, even if they specifically directed those actors not to engage in the actions in question. Indeed, it is likely that this over- and under-inclusiveness has bred much of the disagreement in the doctrine of state responsibility. Faced with the bright line, international judicial bodies are forced to pick a poison—holding a state accountable for nothing or for everything, when the truth likely lies in between. The two bodies that have addressed this issue have found different poisons more palatable.

In the sections that follow, we seek, first, to outline the current approach to state responsibility by the international organizations that have addressed it most prominently. We begin with the ILC’s Draft Articles on States’ Responsibility, which is the most widely embraced description of state responsibility, and yet the most ambiguous. We then turn to the case law of two international judicial bodies, each of which has adopted a different test for state responsibility. The ICJ has embraced the “effective control” test, which draws a very high bar for triggering state responsibility. By contrast, the Appeals Chamber of the ICTY has embraced the “overall control test,” which relies on different elements of control to establish state responsibility. [EN1] We show that it may be possible to reconcile these apparently
contradictory approaches by viewing them as providing two different tests based on whether the state is being held responsible for a non-state actor or for just a single operation by the non-state actor. Yet even accepting this (admittedly minority) approach to making the best sense of existing doctrine, the problem remains that the bright line approach is ill-suited to the project of encouraging states to act in ways that ensure the non-state actors that they support to abide by international law.

A. The ILC’s Draft Articles on State Responsibility

The International Law Commission’s 2001 Draft Articles on State Responsibility are currently the most authoritative statement on state responsibility in international law.\textsuperscript{13} Through the Draft Articles, the ILC sought to clarify and codify the different standards international courts have elaborated for attributing non-state actors’ conduct to states.\textsuperscript{14} In 2007, in \textit{Bosnian Genocide}, the ICJ also declared that both Articles 4 and 8 of the


\textsuperscript{14} See CRAWFORD, supra note 14, at 43–44 (contending that the Draft Articles “are an active and useful part of the process of international law” that codify customary state responsibility).
Draft Articles reflect customary international law.\textsuperscript{15}

Articles 4 and 8 of the Draft Articles are the most significant articles for assessing state responsibility for non-state actor conduct during armed conflict. Under the Draft Articles, a non-state actor’s act is attributable to a state if the state has sufficient connections with the actor (Article 4) or with the operation during which the act takes place (Article 8). Article 4 concerns responsibility for the conduct of non-state actors that can be considered de jure or de facto state organs. Article 8 concerns responsibility for violations committed by non-state actors during an operation that is imputed to a state.

Article 4 of the Draft Articles provides:

1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State.

2. An organ includes any person or entity which has that status in accordance with the internal law of the State.\textsuperscript{16}


\textsuperscript{16} Draft Articles, supra note 13, art. 4.
In its commentary to Article 4, the ILC clarifies that "a State cannot avoid responsibility for the conduct of a body which does in truth act as one of its organs merely by denying it that status under its own law."\textsuperscript{17} Therefore, absent evidence that the non-state actor is a de jure organ of the state, the question under Article 4 boils down to whether the non-state actor is a de facto organ of the state. The Article thus precludes states from avoiding responsibility for a non-state actor that functions as a state organ by simply failing to acknowledge it as such. For instance, a state could not create, fund, and direct a militia, and then use it to evade legal limits on the state’s own actions—for instance, killing civilians in violation of the Geneva Convention’s principle of discrimination. Under Article 4, the actions of the militia would be attributed to the state.

Article 8 of the Draft Articles provides:

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.\textsuperscript{18}

The ILC’s commentary to Article 8 notes that "the three terms ‘instructions’, ‘direction’ and ‘control’ are disjunctive; it is sufficient to

\textsuperscript{17} Draft Articles, supra note 13, art. 4, cmt. 11. [EN2]

\textsuperscript{18} Draft Articles, supra note 13, art. 4.
establish any one of them.” Therefore, absent express instructions or direction from the state to the non-state actor to commit the act, the question boils down to whether the state exercised a sufficient degree of “control” over the act. The focus of the inquiries under Article 4 and Article 8 is therefore different. Under Article 4, the question is the level of control the state exercises over the actor that undertakes the act, whereas under Article 8, it is the level of control the state exercises over the operation during which the act occurs.

While some commentators have suggested that “the ILC sought to allow for greater state responsibility under the Articles as adopted,” most recognize the Draft Articles as codifying and clarifying the applicability of pre-existing judicial tests for state responsibility. The most prominent

19. *Id.* at art. 8, cmt. 7.

20. See Dayna L. Kaufman, *Don’t Do What I Say, Do What I Mean: Assessing a State’s Responsibility for the Exploits of Individuals Acting in Conformity with a Statement from a Head of State*, 70 FORDHAM L. REV. 2603, 2653 (2002) (“[C]hanges in the Articles on State Responsibility from their original draft form to their form as adopted suggest that perhaps the ILC sought to allow for greater state responsibility under the Articles as adopted. Additionally, there is greater interest internationally in holding States responsible for their conduct with respect to private individuals, as evinced by recent General Assembly resolutions regarding terrorism.”) (citations omitted).

21. See CRAWFORD, *supra* note 13, at 43–44 (describing the Draft Articles as “an accurate codification of the customary international law of state responsibility”). The ILC adopted the most recent version of the *Draft Articles* in August 2001—after the ICJ’s 1986 Judgment in *Nicaragua* and the ICTY’s Tadić Appeals Chamber decision, but before the ICJ’s repudiation of the ICTY’s
judicial tests for state responsibility are the “effective control” test of the International Court of Justice and the “overall control” test of the International Criminal Tribunal for the Former Yugoslavia. It is therefore to those that we turn next.

B. The ICJ’s Effective Control Test

The International Court of Justice was the first to confront the problem of state responsibility for non-state actors. It responded by creating a new legal standard for finding of state responsibility: If an applicant could prove that a state had sufficiently close ties to, and had furnished sufficient support for, a non-state actor, courts would attribute the non-state actor’s actions to the state—essentially “piercing the veil” of the proxy relationship.

In 1984, in Military and Paramilitary Activities in and Against Nicaragua (Nicaragua), Nicaragua instituted proceedings against the United States for its use of the contras—a non-state armed group operating in and around Nicaragua—to fight the socialist Sandinista government.


Nicaragua alleged, and the ICJ found, that the United States was directly responsible for the internationally wrongful act of mining Nicaraguan ports.\textsuperscript{23} However, Nicaragua also alleged indirect U.S. involvement—via training, financing, and direction provided to paramilitaries—in other internationally wrongful acts carried out by the \textit{contras}.\textsuperscript{24}

The ICJ found that the United States had supported the \textit{contras} in the following ways:

The United States financed, organized, trained, supplied, equipped, and armed the \textit{contras}, and provided them with reconnaissance aircraft, intelligence, and surveillance.\textsuperscript{25}

The United States decided and planned—or at least closely collaborated in deciding and planning—a number of military and paramilitary operations by the \textit{contras},\textsuperscript{26} and devised and directed specific strategies and tactics on when to seize and hold territory.\textsuperscript{27} In addition, the United States selected some of the \textit{contras}' military and paramilitary targets and provided

\begin{itemize}
  \item \textit{Id.} \textsuperscript{¶} 292(4).
  \item \textit{Id.} \textsuperscript{¶¶} 100–01, 104, 106, 108, 112, 115, 118–19, 122.
  \item \textit{Id.} \textsuperscript{¶¶} 100–01, 108, 115.
  \item \textit{Id.} \textsuperscript{¶} 106.
  \item \textit{Id.} \textsuperscript{¶} 104. It is not clear whether the alleged violations of human rights and humanitarian law occurred in the course of these operations.
\end{itemize}
operational support.28

The United States prepared and distributed a manual suggesting that the *contras* shoot civilians attempting to leave a town, neutralize local judges and officials, hire professional criminals to carry out “jobs,” and provoke violence at mass demonstrations to create “martyrs.”29 In other words, the United States “encouraged” the commission of unlawful acts.30

But in deciding what legal consequences should follow from these actions, the Court faced more than simply a legal challenge. After it found that it had jurisdiction, the United States not only withdrew from the case, but it also withdrew its optional declaration accepting the compulsory jurisdiction of the Court.31 As a result, the Court was under significant pressure to deliver a judgment that, on the one hand, asserted its jurisdiction despite the withdrawal of the United States, and, on the other, was limited

---

28. *Id.* ¶¶ 112, 115.

29. *Id.* ¶¶ 118–19, 122.

30. *Id.* ¶ 292(9).

enough in scope that it would not undermine the legitimacy of the Court in the event the United States decided to flout the final ruling.

Likely as a result of this politically sensitive situation, the Court drew a bright line that established a high bar for state responsibility. It concluded that in order for a state to be held responsible for the actions of a non-state actor, “It would in principle have to be proved that that State had \textit{effective control} of the military or paramilitary operations in the course of which the alleged violations were committed.”\textsuperscript{32} Under this “effective control” standard, a later case clarified, private conduct that is merely supported, financed, planned, or otherwise carried out on behalf of the state is not attributable unless the state also exercises a high level of control “in respect of each operation in which the alleged violations occurred.”\textsuperscript{33}

Applying this standard, the ICJ found that the combination of funding, training, public support, strategic guidance, and tactical directives cited above was insufficient for a finding of state responsibility.\textsuperscript{34} The opinion implied that this was because Nicaragua had failed to prove a direct link between these forms of support and the execution of any particular operation, i.e., the United States had not specifically \textit{instructed} the commission of

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{32} Nicaragua, 1986 I.C.S., ¶ 115 (emphasis added).
\item \textsuperscript{33} Bosnia Genocide, 2007 I.C.J., ¶ 400 (emphasis added).
\item \textsuperscript{34} Nicaragua, 1986 I.C.J., ¶¶ 103–07, 115.
\end{enumerate}
\end{footnotesize}
unlawful acts. The ICJ took pains to note that proof of control over a specific operation was required for a finding of attribution.

Practically, this meant that unless the plaintiff could provide evidence directly connecting a state’s funding, training, and tactical or strategic guidance to the execution of a discrete internationally wrongful act, there could be no finding of attribution. In other words, the test set a high evidentiary bar, particularly in the context of a contentious case, where evidence indicative of the kind of control required over a specific operation would generally be classified and in exclusive control of the state.

35. *Bosnian Genocide*, 2007 I.C.J., ¶ 400 (“It must . . . be shown that this ‘effective control’ was exercised, or that the State’s instructions were given, in respect of each operation in which the alleged violations occurred . . . .” (emphasis added)); *Nicaragua*, 1986 I.C.J., ¶ 115 (“For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.” (emphasis added)).

36. The ICJ later explicitly affirmed the requirement of control over a specific operation in *Bosnian Genocide. Bosnian Genocide*, 2007 I.C.J., ¶ 400 (“It must . . . be shown that this ‘effective control’ was exercised, or that the State’s instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.” (emphasis added)). The requirement of control over a specific operation is the major factor that distinguishes the ICJ’s effective control test from the ICTY’s overall control test. The evidentiary threshold of the ICTY’s test is easier to clear—once it is proved that material support has flowed to an actor, this may provide the basis for a finding of control over the actor.

37. Although the ICJ has the authority to compel states to produce documents under Article 49
In its 2007 judgment in *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnian Genocide)*, the ICJ confirmed the effective control test and again applied it in a way that indicated that it established a high evidentiary burden to find attribution. The case raised the question of whether the acts of military and paramilitary groups operating on the territory of the Former Republic of Yugoslavia (FRY) could be attributed to the government in the period before its disintegration in the early 1990s. Specifically, the suit alleged that the murder of Bosnian Muslim men and boys at Srebrenica by members of the Republika Srpska’s official military wing, the Bosnian Serb Army (VRS), should be attributed to the FRY. (At the time, Republika Srpska was an unrecognized breakaway republic and therefore did not yet bear its own legal responsibilities as a state.)

The ICJ found that the FRY was “making . . . considerable military and financial support available to the Republika Srpska, and had it withdrawn that support, this would have greatly constrained the options” of the breakaway

---

of its statute, in *Bosnian Genocide*, the Court declined to order Serbia to produce unredacted versions of state documents that incriminated Belgrade in the Srebrenica genocide. See *Bosnian Genocide*, 2007 I.C.J., ¶ 35 (Dissenting opinion by Al-Khasawneh, V.P.).


40. *Id.* ¶¶ 278–88.
republic's authorities.\textsuperscript{41} The ICJ furthermore determined that there were “close ties” between the government of the FRY and officials of the Republika Srpska; there had been a major transfer of personnel, arms and equipment from the army of the FRY to the VRS, as well as financial support from FRY authorities to VRS officers; and, furthermore, there was substantial economic integration between the Republika Srpska and the FRY (among other things, loans from the FRY underwrote most of the budget of the breakaway republic).\textsuperscript{42}

Despite these ties, the ICJ held that while Bosnia and Herzegovina had proven that FRY had supported the VRS and the Republika Srpska and that the VRS’s acts at Srebrenica had been acts of genocide, it had failed to prove that the acts of the VRS were attributable to the FRY under the effective control test.\textsuperscript{43} Explaining its decision, it wrote:

The Applicant has not proved that instructions were issued by the federal authorities in Belgrade, or by any other organ of the FRY, to commit the massacres, still less that any such instructions were given with the specific intent (\textit{dolus specialis}) characterizing the crime of genocide.... All indications are to the contrary: that the decision to kill the adult male population of the Muslim community in Srebrenica

\textsuperscript{41} Id. ¶ 241.

\textsuperscript{42} Id. ¶¶ 237–40.

\textsuperscript{43} Nor could any of the acts alleged that did not amount to genocide be attributed to the FRY.
was taken by some members of the VRS Main Staff, but without instructions from or effective control by the FRY.\textsuperscript{44}

Here, the ICJ appeared to require evidence of explicit instructions to commit the massacre—and even evidence of genocidal intent\textsuperscript{45}—in order to meet the effective control standard. By requiring evidence of specific instructions tied to a particular operation, the ICJ set an extremely high bar for attribution.

Because the ICJ did not find effective control in either \textit{Nicaragua} or \textit{Bosnian Genocide}, it is unclear exactly what set of facts would satisfy the “effective control” test. However, it is clear that it sets a high threshold.\textsuperscript{46}

\begin{flushright}
\textsuperscript{44} \textit{Bosnian Genocide}, 2007 I.C.J. 3, ¶ 413.
\end{flushright}

\begin{flushright}
\textsuperscript{45} Although the necessity of finding intent likely also was exacerbated by the \textit{dolus specialis} requirements of the crime of genocide. \textit{See e.g.}, Kai Ambos, \textit{What Does ‘Intent to Destroy’ in Genocide Mean?}, 91 INT’L REV. RED CROSS 833, 834(2010) (Laying out the two separate mental elements of the genocide offense).
\end{flushright}

\begin{flushright}
\textsuperscript{46} The \textit{Bosnian Genocide} opinion suggests that to satisfy the effective control test there must be evidence a state directly instructed a non-state group to carry out the specific operation during which the violation took place. \textit{Bosnian Genocide}, 2007 I.C.J., ¶¶ 408, 410–12. This appears to set a higher evidentiary standard than the ILC proposes in the Draft Article commentaries for Article 8. In its formulation of the factors required to establish effective control, the ILC treats the terms “instructions,” “directions,” and “control” as disjunctive. \textit{Id.}, ¶ 399. The commentaries thus suggest that directions, instructions, or control are independently sufficient for a finding of state responsibility under Article 8. In the ICJ’s formulation of the same factors, however, the court reads “instructions” back into the control test, so that instructions are \textit{always} necessary for a finding of
\end{flushright}
Hypothetically, a state’s use of a non-state actor to carry out a targeted killing would constitute an exercise of effective control over a non-state actor. Yet, the state’s involvement would likely have to entail significant control over the military operation—at the very least, it would have to exceed that exercised by the United States over the contra or the FRY over the VRS. The ICJ’s reasoning in Nicaragua and Bosnian Genocide might be read to suggest that a state could arm, fund, support, train, and facilitate the operations of an armed non-state group, and even encourage the non-state group to carry out ethnic cleansing as a means of defeating the enemy, and nevertheless evade responsibility because there is no evidence state agents directly instructed the commission of the specific massacre.

However, the ICJ has ultimately left the question of state liability for ultra vires actions underspecified. “Effective control” appears to contemplate state responsibility for an ultra vires act by a non-state actor in limited circumstances. In both Nicaragua and Bosnian Genocide, the ICJ held that the state needs to have “effective control” over the operation during effective control. Id., ¶ 413. Under this standard, courts may even have the flexibility to construe the term operation so narrowly as to foreclose the possibility of holding a state responsible for the ultra vires actions of its non-state partners.

47. A similar analysis might apply in a case involving an unorganized group of individuals carrying out specific operations on behalf of a state. If the non-state actor does not meet the Tadić threshold of organization, non-state actors must meet effective or strict control for state attribution to obtain.
which the violations occur in order to trigger a finding of attribution under this standard—mentioning nothing about control over the acts (or violations) themselves. The choice to focus the inquiry on control over the operation, rather than the act, suggests that a state could be held responsible for ultra vires acts that take place in the course of an operation over which that state exercises effective control.

By contrast, the ILC, which endorses the ICJ’s “effective control” standard (as articulated in Nicaragua), limits liability for ultra vires acts during operations over which a state exercises “effective control” to those that are “an integral part” of the operation. It does not extend responsibility to ultra vires acts that are only “incidentally or peripherally” associated with an operation. It explains that “[s]uch conduct will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation.” It further explains, “The principle does not extend to conduct which was only incidentally or

48. Nicaragua, 1986 I.C.J. 14, ¶ 115 (June 27) (“For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.”); Bosnian Genocide, 2007 I.C.J., ¶ 400.

49. Draft Articles, supra note 17, art. 8, cmt. 4. [EN5]

50. Id.

51. Id.

52. Id.
peripherally associated with an operation and which escaped from the State’s direction or control.”  

Indeed, some language in *Bosnian Genocide* and *Nicaragua* suggests that a state by definition does not have “effective control” over an *ultra vires* act. In other words, to attribute an act of a non-state actor to a state under the “effective control” standard, the state must have instructed or directed the specific act that constitutes the violation in question.

53. *Id.*

54. *Bosnian Genocide*, 2007 I.C.J., ¶ 400 (“It must however be shown that this ‘effective control’ was exercised, or that the State’s instructions were given, in respect of each operation in which the alleged violations occurred . . .”). One could interpret the “or” in this sentence as an explanatory word. *Nicaragua*, 1986 I.C.J., ¶ 115 (“All the forms of United States participation [and control] mentioned above . . . would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State.”). One could interpret this sentence to mean that “direction” and “enforcement” are necessary to find the state responsible.

55. This depends on how one defines “operation.” If the term “operation” is narrowly construed to mean that each act that makes up an operation must be directed by the state (*Tadić*’s reading), then the state cannot be held responsible for acts that were not expressly instructed by the state. However if “operation” is construed so that several acts are steps in one operation, then it is possible to be responsible for an *ultra vires* act under the ILC reading as long as the act in question is integral to the operation ordered by the state. The Appeals Chamber of the ICTY in *Tadić* appears to have interpreted *Nicaragua* and *Bosnian Genocide* in this manner. *See Tadić*, Case No. IT-94-1-A, Appeals Chamber, Judgment, ¶ 106 (Int’l Crim. Trib. for the Former Yugoslavia July 15, 1999) (“This [effective control] test hinged on the issuance of specific directives or instructions concerning
In sum, the ICJ’s application of effective control risks narrowing the scope of accountability to the point of rendering state responsibility doctrine ineffective. In *Nicaragua* and *Bosnian Genocide*, “effective control” requires such a high-degree of control and specificity of instructions that states can—merely by issuing instructions at a relative level of generality—easily avoid attribution for crimes as egregious as genocide.

The International Court of Justice’s approach to state responsibility thus leaves many unanswered questions. It does permit the actions of non-state actors to be attributed to states—and in this respect partially addressed the legal loophole created by the possibility of states acting through non-state actors. But it adopted a strict liability rule that sets a very high evidentiary bar for triggering state attribution. In doing so, the Court left a substantial accountability gap that, taken alone, would permit states to escape legal limits on their own actions by encouraging and enabling non-state actors to take action on their behest.

C. The ICTY’s Overall Control Test

Eleven years after the ICJ’s ruling in *Nicaragua*, the International Criminal Tribunal for the Former Yugoslavia also confronted the question of state attribution in *Prosecutor v. Dusko Tadić*. In the case, the prosecutor

the breaches allegedly committed by the contras.”

56. *Id.* § 131.
brought a criminal suit against Dusko Tadić, a Bosnian Serb politician and member of a paramilitary group, for “grave breaches” of international humanitarian law.\textsuperscript{57}

Because it was a criminal case, the stakes of a finding of attribution in \textit{Tadić} were somewhat different than in \textit{Nicaragua}. In particular, finding Tadić guilty hinged on whether international humanitarian law applied to the parties to the conflict. After all, Tadić was charged with violating international humanitarian law that applies during international armed conflict—a charge that could only hold if the law was applicable to the conflict. The ICTY’s ability to find criminal liability thus hinged on the attribution of paramilitary conduct against the state of Bosnia and Herzegovina to a second state, the Federal Republic of Yugoslavia (FRY)—an attribution that would make the conflict an international armed conflict and would thereby trigger the full panoply of international humanitarian laws applicable to such conflicts.

The threshold question was whether the acts of the Republika Srpska’s army (the VRS) could be attributed to the FRY. Since, as noted earlier, Republika Srpska was not a recognized state, the conflict between Republika Srpska and Bosnia Herzegovina—in which Tadić committed his offenses—was not an international armed conflict. However, if the acts of the Republika

\textsuperscript{57} \textit{Id.} ¶ 68.
Srpska’s army (the VRS) could be attributed to the Federal Republic of Yugoslavia (a recognized state), then the conflict would be an international armed conflict between two states (the FRY and Bosnia and Heregovina). Members of the VRS could thus be held accountable for the atrocities committed during the war under the stricter standards of conduct that international humanitarian law imposes on participants in international armed conflicts.58

58. This question came before the ICTY in 1995. Id. ¶ 7. Article 2 of the ICTY Statute empowers the Tribunal to “prosecute persons committing or ordering to be committed grave breaches of the Geneva Conventions,” including crimes that only arise in the course of an IAC. Id. ¶ 577. Since the prosecution indicted Dusko Tadić for conduct that only constitutes a breach of the Geneva Conventions under IAC–IHL rules, the ICTY had to determine whether there was an IAC. In order to satisfy the elements required to establish grave breaches of the Geneva Conventions—for Bosnian-Muslims to be considered “protected persons” within the meaning of the Geneva Conventions—the prosecution had to show that the victims were in the hands of a party to the conflict of which they were not nationals (i.e., that the VRS perpetrators were agents or organs of the Former Republic of Yugoslavia). In Tadić, the Trial Chamber recognized that there was an IAC before May, 19 1992. Id. ¶ 607. It held, however, with the presiding judge dissenting, that although “the JNA played a role of vital importance in the establishment, equipping, supplying, maintenance and staffing of the . . . VRS units,” the VRS were not organs or agents of the FRY. Id. ¶¶ 595, 608. As a result, the Trial Chamber concluded that there was not an IAC, and so Tadić could not be found guilty of any of the counts post-dating May 19, 1992 that relied on Article 2 of the ICTY Statute. Id. ¶ 608. The Prosecutor appealed this part of the judgment, claiming that even after May 19 there was an IAC between the FRY and BH. Id. ¶ 85. The Prosecutor argued that only IHL (and not the law of State responsibility) should be used to determine whether Article 2 of the Statute applies. Id.
The Appeals Chamber explicitly rejected the application of the Nicaragua “effective control” test to the facts of the case.\textsuperscript{59} It noted that the purpose of Article 8 of the Draft Articles—an earlier version of which had been adopted by the ILC drafting committee in 1998—was “to prevent States from escaping international responsibility by having private individuals carry out tasks that may not or should not be performed by State officials.”\textsuperscript{60} As a result, it declared that “the degree of control [required for attribution] may . . . vary according to the factual circumstances of each case.”\textsuperscript{61} In particular, it observed that for organized groups, “it is sufficient to require that the group as a whole be under the overall control of the State.”\textsuperscript{62}

In explaining this new overall control test, the Appeals Chamber clarified that the State must not only “equip[] and financ[e]” the group, but also “coordinat[e] or help[] in the general planning of its military activity.”\textsuperscript{63}

\textsuperscript{59} Id. \S 115.
\textsuperscript{60} Id. \S 117.
\textsuperscript{61} Id.
\textsuperscript{62} Id. \S 120 (emphasis added).
\textsuperscript{63} Id. \S 131; see also id. \S 137 (“The control required by international law may be deemed to exist when a State (or, in the context of an armed conflict, the Party to the conflict) has a role in organising, coordinating or planning the military actions of the military group, in addition to
Distinguishing the ICJ’s effective control standard, the Appeals Chamber emphasized that the overall control test does not go so far as to require “the issuing of specific orders by the State, or its direction of each individual operation.”

In applying the test to the facts, the Appeals Chamber found that the FRY exercised overall control over the VRS. It emphasized that:

- JNA (SFY) officers were directly transferred into their equivalent postings in the VRS;
- the FRY/VJ paid the salaries of these officers;
- the VJ had the same military objectives as the VRS;
- the FRY/VJ provided “extensive financial, logistical and other assistance and support” to the VRS; and
- the FRY/VJ “directed and supervised the activities and operations of the VRS.”

The Appeals Chamber concluded that the VJ and the

financing, training and equipping or providing operational support to that group.”

64. *Id.* ¶ 137.
65. *Id.* ¶ 147.
66. *Id.* ¶ 150.
67. *Id.*
68. *Id.* ¶ 151.
69. *Id.*
70. *Id.*
VRS “did not, after May 1992, comprise two separate armies in any genuine sense.”71

The Appeals Chamber held that there was an IAC, and that Tadić was therefore liable for grave breaches of the Geneva Conventions under CA2 and Article 2 of the ICTY Statute.

By using the overall control standard, the ICTY Appeals Chamber was able to apply international humanitarian law applicable to international armed conflicts to the facts of Tadić and reject efforts to evade international criminal responsibility. Ultimately, the Appeals Chamber held that in cases involving organized armed military groups, evidence the state exercised a more general level of control over the non-state group is sufficient to attribute the groups’ conduct to a state.

Moreover, the overall control test, as articulated by the ICTY, is a strict liability standard: Once a non-state actor is considered to be under the overall control of a state, the state is responsible for all acts, including ultra vires acts carried out by the non-state actor.72 If the test is regarded as a test for whether a group is functionally an organ of the state, this standard makes intuitive sense. There is little question that a state is responsible for an ultra vires act committed by its de facto organ. Article 7 of the Draft Articles provides:

71. Id.

72. Id. ¶¶ 120–22.
"The conduct of an organ of a State . . . shall be considered an act of the State under international law . . . even if [the organ] exceeds its authority or contravenes instructions."\textsuperscript{73} The ILC Commentary also points to an abundance of state practice and judicial decisions supporting this notion.\textsuperscript{74} In fact, both the ICJ\textsuperscript{75} and the Appeals Chamber of the ICTY\textsuperscript{76} have come to a similar conclusion.

Indeed, many scholars have praised the overall control test precisely because it adopts a more capacious test for establishing state responsibility for the actions of non-state actors. The ICRC has expressly endorsed the overall control test as the appropriate standard in armed conflict, not only for purposes of classifying the conflict, but also for attributing state responsibility for the conduct of non-state actors.\textsuperscript{77} Commentators have also

\begin{itemize}
\item \textsuperscript{73} Draft Articles, supra note 13, art. 7.
\item \textsuperscript{74} Id. at art. 7, cmts. 1–8.
\item \textsuperscript{75} Nicaragua, 1986 I.C.J., ¶ 109; Bosnian Genocide, 2007 I.C.J., ¶¶ 385–86.
\item \textsuperscript{76} Tadić, Case No. IT-94-1-A, ¶ 121.
\item \textsuperscript{77} Acknowledging that the ICTY’s overall control test is the minority position, the ICRC nevertheless contends that it is the appropriate test in armed conflicts for several reasons. “In order to classify a situation under humanitarian law involving a close relationship, if not a relationship of subordination, between a non-State armed group and a third State, the overall control test is appropriate because the notion of overall control better reflects the real relationship between the armed group and the third State, including for the purpose of attribution. It implies that the armed group may be subordinate to the State even if there are no specific instructions given for every act of belligerency. Additionally, recourse to the overall control test enables the assessment of the level
\end{itemize}
noted the utility of the lower standard of attribution in the context of state-sponsored terrorism,\textsuperscript{78} private military and security contractors,\textsuperscript{79} and non-state paramilitary groups.\textsuperscript{80}

of control over the \textit{de facto} entity or non-State armed group as a whole and thus allows for the attribution of several actions to the third State. Relying on the effective control test, on the other hand, might require reclassifying the conflict with every operation, which would be unworkable. Furthermore, the test that is used must avoid a situation where some acts are governed by the law of international armed conflict but cannot be attributed to a State.” ICRC, \textit{supra} note 11, art. 3, ¶ 409 (2016).


\textbf{80. Moyakine, supra} note 78, at 274; \textit{see id.} at 281–82 ("[T]he ‘overall control’ test appears
Despite these advantages, the ICTY’s overall control test has not been widely embraced. Instead, the effective control standard is regarded by many observers as the governing standard.\textsuperscript{81} In updating the Draft Articles, the ILC expressly supported the ICJ’s effective control standard in the final text and commentary, leaving its assessment of the overall control test’s viability ambiguous.\textsuperscript{82} In the 2007 \textit{Bosnian Genocide} case, moreover, the ICJ rejected to be the most suitable one, while States, especially those hiring PMSCs (which can be equated with paramilitary units), are likely to easily satisfy the set of criteria for the application of this test. It will automatically lead to the attribution of their unlawful conduct to the States concerned if the reasoning of the ICTY positioning its control theory as realistic is followed.”); Cassese, \textit{supra} note 78, at 657–58, 665.

\textsuperscript{81} See CRAWFORD, \textit{supra} note 13, at 156 (“The ICJ’s determination in \textit{Bosnian Genocide} effectively ends the debate as to the correct standard of control to be applied under Article 8. Moreover it does so in a manner that reflects the ILC’s thinking on the subject from the time the term ‘control’ was introduced into then-Draft Article 8.”); MOYAKINE, \textit{supra} note 78, at 269 (“[O]ne can draw the conclusion that the ‘effective control’ test is the leading theory according to the World Court.”); Christian J. Tams, \textit{Law-making in Complex Processes: The World Court and the Modern Law of State Responsibility, in Sovereignty, Statehood and State Responsibility: Essays in Honour of James Crawford} 287, 301 (Christine Chinkin & Freya Baetens eds., 2015) (“As a result, it would seem far-fetched today to suggest that overall control is sufficient to justify attribution of private conduct—faced with dissent the ILC-ICTY has struck back.”).

\textsuperscript{82} See Draft Articles, \textit{supra} note 13, at 47–48 (noting that the degree of control was analyzed by ICJ and it rejected the broader claim of \textit{Nicaragua} that all the conduct of the contras was attributable to the United States by reason of its control over them).
the overall control standard and reaffirmed the effective control standard it had first established in *Nicaragua*. Unbowed, the ICTY has since reaffirmed the overall control standard on at least two occasions.

Commentators generally present the ICJ’s “effective control” and the ICTY’s “overall control” standards as alternatives. And in many ways, they are: the ICJ and the ICTY each explicitly rejected the other court’s approach after characterizing the tests as standards of attribution under Article 8 of the Draft Articles. In *Tadić*, the ICTY criticized the ICJ’s “effective control”

---

83. While the ICJ acknowledged that “overall control” may well be the appropriate standard for determining whether or not an armed conflict is international or not, the Court rejected its application in the context of state responsibility doctrine. Bosnian Genocide, 2007 I.C.J., ¶¶ 403–07. *But see id.* ¶ 39 (Dissenting opinion by Al-Khasawneh, V.P.) (“The inherent danger in [the effective control test] is that it gives States the opportunity to carry out criminal policies through non-state actors or surrogates without incurring direct responsibility therefore.”).

84. *See, e.g.*, Prosecutor v. Delalic, Case No. IT-96-21-A, Appeals Chamber, Judgment, ¶ 26 (Int’l Crim. Trib. for the Former Yugoslavia Feb. 20, 2001) (confirming that the “overall control” standard articulated in *Tadić* was the applicable criteria in ascertaining the existence of an international armed conflict); Prosecutor v Aleksovski, Case No IT-95-14/1-A, Appeals Chamber, Judgment, ¶ 137 (Int’l Crim. Trib. for the Former Yugoslavia Mar. 24, 2000) (holding that the question of Yugoslavia’s responsibility for the acts of Bosnian Serb forces was subject to an “overall control” test).

85. *See, e.g.*, CRAWFORD, supra note 13, at 156 (noting that the effective control test sets the bar too high and the test of overall control would better meet the needs of the international community in dealing with the threat of terrorism); Tams, supra note 80, at 301 (noting that both ICJ and ILC were robust in defending effective control test against ICTY’s overall control test).
standard from *Nicaragua* and proposed the “overall control” standard to replace it in cases where the non-state actor is an organized group.  

Responding in *Bosnian Genocide* to the ICTY’s appraisal, the ICJ criticized the ICTY’s “overall control” standard and reaffirmed the “effective control” standard it had first established in *Nicaragua* (notwithstanding the non-state actor’s level of organization). In the commentary on Article 8, meanwhile, the ILC itself took note of the dispute between the ICJ and ICTY. But the ILC leaves room for reconciliation. The Draft Articles favorably cite the effective control test and note that the ICTY’s mandate was directed toward

---

86. See *Tadić*, Case No. IT-94-1-A, ¶ 123 (“In the case under discussion here, that of organised groups, State responsibility is instead the objective corollary of the overall control exercised by the State over the group. . . . [T]he fact nevertheless remains that international law renders any State responsible for acts in breach of international law performed (i) by individuals having the formal status of organs of a State (and this occurs even when these organs act *ultra vires or contra legem*), or (ii) by individuals who make up organised groups subject to the State’s control. International law does so regardless of whether or not the State has issued *specific instructions* to those individuals. Clearly, the rationale behind this legal regulation is that otherwise, States might easily shelter behind, or use as a pretext, their internal legal system or the lack of any specific instructions in order to disclaim international responsibility.”).

87. While the ICJ acknowledged that “overall control” may well be the appropriate standard for determining whether or not an armed conflict is international or not, the Court rejected its application in the context of state responsibility doctrine. *Bosnian Genocide*, 2007 I.C.J., ¶¶ 403–07.

“issues of individual criminal responsibility, not state responsibility,” but the ILC does not expressly reject the overall control test.89

In sum, in the context of armed conflict, the ICJ and the International Criminal Tribunal for the Former Yugoslavia (ICTY) have relied primarily on two90 standards for evaluating the level of control required to attribute an act of a non-state actor to a state under the Draft Articles: effective control and overall control. These two tests have traditionally been understood as mutually inconsistent. Yet it is possible to see them as reconcilable.

89. Draft Articles, supra note 13, art. 8, cmt. 5. The ILC’s commentary has itself been the subject to significant scholarly debate. The ILC concludes its assessment of the ICJ and ICTY’s disagreement by noting that “it is a matter of appreciation in each case whether particular conduct was or was not carried out under the control of a State, to such an extent that the conduct controlled should be attributed to it. Id. at 112.

90. The ICJ also articulated the additional “strict control” standard, which establishes that all of the acts of a non-state actor are attributable to a state if that non-state actor is in a relationship of “complete dependence” on the state. Bosnian Genocide, 2007 I.C.J., ¶ 391 (asking “whether it is possible in principle to attribute to a State conduct of persons — or groups of persons — who, while they do not have the legal status of State organs, in fact act under such strict control by the State that they must be treated as its organs for purposes of the necessary attribution leading to the State’s responsibility” (emphasis added)). In Nicaragua, the court uses the phrase “complete dependence” to refer to the same control standard. Nicaragua, 1986 I.C.J., ¶ 110. The “strict control” standard is, on our view, the most stringent (i.e., the most difficult for establishing attribution). Under strict control the accountability gap is therefore also widest. Given our critique of the limitations of the arguably less high evidentiary burdens of effective and overall control, we do not discuss strict control in detail in this paper.
According to the ICJ in *Nicaragua*, an act of a non-state actor is attributable to a state if the state exercises “effective control” over the operation during which the act occurred.91 Under the effective control standard, private conduct that is merely supported, financed, planned, or otherwise carried out on behalf of the state is not attributable unless the state also exercises a high level of control “in respect of each operation in which the alleged violations occurred.”92 According to the ICTY in its *Tadić* appeals judgment, however, in cases where the non-state actor is an organized military group, the state only needs to exercise overall control over the *actor* for the act to be attributable to the state.93 As long as the non-state actor is organized, evidence that the state financed and equipped a “military organization” and participated in the general planning of the group’s operations is sufficient to establish state responsibility, even if the state did not issue specific instructions.94

91. *Nicaragua*, 1986 I.C.J., ¶ 115 (“For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.”).

92. *Bosnian Genocide*, 2007 I.C.J., ¶ 400 (emphasis added). Admittedly, it is difficult to ascertain the exact content of the effective control standard—thus far no court or tribunal has found sufficient evidence of effective control to trigger state responsibility.

93. *Tadić*, Case No. IT-94-1-A, ¶ 131 (“In order to attribute the acts of a military or paramilitary group to a State, it must be proved that the State wields overall control over the group . . . .”).

94. *Id.* ¶ 145 (“In the case at issue, given that the Bosnian Serb armed forces constituted a
These two approaches, moreover, might be seen as reflected in the ILC Draft Articles, the overall control test addressing attribution under Article 4 and the effective control test addressing attribution under Article 8. Indeed, a handful of commentators have suggested that the "overall control" standard is best understood in terms of the legal theory of attribution underlying the ICJ’s control standard under Article 4, rather than under Article 8.95 Indeed, this understanding of the relationship between the standards adopted by the ICJ and the ICTY on the one hand, and the Draft Articles on the other, might

‘military organization’, the control of the FRY authorities over these armed forces required by international law for considering the armed conflict to be international was overall control going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations. By contrast, international rules do not require that such control should extend to the issuance of specific orders or instructions relating to single military actions, whether or not such actions were contrary to international humanitarian law.”).

even make the best sense of current state responsibility doctrine.\footnote{The Draft Articles Commentary discusses overall control as a standard of attribution under Article 8. Draft Articles, supra note 17, art. 8, cmt. 5. Nevertheless, a close reading of Tadić reveals that the overall control standard assesses whether the conduct of the non-state actor can be attributed to the state by virtue of the control it exercises over the group (Article 4), rather than the specific operation (Article 8). In Tadić, because the Appeals Chamber found the non-state armed group to be a de facto state organ, it classified the conflict as an international armed conflict (effectively between two states) rather than a non-international armed conflict (between a state and a non-state group). Like standards of attribution under Article 4, once the conduct of the state in this case met the overall control threshold, all of the conduct of the non-state actor could be attributed to it, regardless of whether the state had exercised a high level of control over particular operations. In this sense, the overall control inquiry asks whether the armed group in question can be attributed to the state, and with it, all of the non-state actor’s conduct.}

Regardless of the standard, however, all these approaches share a common vice: By drawing a bright line, they force a difficult—if not impossible—decision as to how much control over a non-state actor is enough to hold a state responsible for its actions. On the one hand, drawing the line for triggering state responsibility too high allows states to easily evade legal limits on their own actions. On the other hand, drawing it too low can threaten to place states in an unfair position of being held liable for actions they could not reasonably prevent. Both approaches, moreover, allow states to avoid responsibility for taking actions that enable non-state actors to violate international law, as long as they stay far below the bar.

In the next Part, we examine more fully the incentives that modern
attribution doctrine creates for states, before turning in Part III to elaborating a possible solution presented by Common Article 1 to the Geneva Conventions.

II. Perverse Incentives

The bright-line approach to state responsibility that characterizes modern attribution doctrine creates perverse incentives for states. First, the high bar established by state responsibility doctrine may encourage states to use non-state partners to undertake actions that are prohibited to the states themselves. This may be true even under the more capacious overall control standard, for even that standard requires a significant level of state control over the non-state actor before triggering responsibility. Second, the doctrine may encourage states to hold non-state actors at arm’s length—for instance providing them weapons but little training or instructions on compliance with international humanitarian law—for fear that closer involvement might trigger attribution. This is particularly true for those concerned about how the overall control test may be applied, for that test creates a greater likelihood that the state could be held responsible even for ultra vires actions.

A. The Incentive to Use Non-State Actors to Violate International Law

Consider the following possibility: Suppose a state supports a non-state group seeking to overthrow its government. (This is no mere hypothetical: Think, for example, of the many states supporting various non-state groups
at war in Syria.) The state would like to assure the victory of the side it supports, but it would also like to avoid any responsibility for violations of international law. It also knows that it would be prevented from sending in its own troops unless the government of Syria were to give its permission—unlikely if the non-state group it supports is seeking to topple the government. Due to *jus ad bellum* concerns and domestic legal and political limits on sending in the troops, the state may already prefer to send non-state actors instead of its own armed forces. 97 Because of the high bar established by modern attribution doctrine, states in this circumstance may believe that they can work through non-state actors and thereby avoid legal responsibility that would be triggered if they employed their own forces.

It is undisputed that any and all acts of the state’s armed forces would

---

97. States working through non-state actors are not immune from *jus ad bellum* constraints. The *Nicaragua* Court found that “the mere supply of funds to the *contras*, while undoubtedly an act of intervention in the internal affairs of Nicaragua, as will be explained below, does not in itself amount to a use of force.” It nonetheless indicated that “‘organizing or encouraging the organization of irregular forces or armed bands . . . for incursion into the territory of another State’ and ‘participating in acts of civil strife . . . in another State’” could, in some circumstances, violate the customary law prohibition on use of force. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. 14, ¶ 228 (June 27). [EN6] The potential violation of Article 2(4) of the U.N. Charter was not before the Court, but the same logic would suggest that this prohibition applies to the overlapping Charter provision on the use of force. See *id.*
be attributable to the state. Under Article 4 of the Articles on State Responsibility, the armed forces of a state are widely considered “organs” of the state.\textsuperscript{98} Therefore, any and all acts committed by the armed forces, even if \textit{ultra vires}, could be attributed to the state. So if a state’s soldier goes rogue and commits war crimes, the state would be directly responsible (a responsibility it could discharge by court martialing the offender).

Moreover, the rules of international law governing the conduct of the state’s armed forces impose substantial risks and burdens on the state. If a state sends its own armed forces, their conduct is more likely to be governed by the law that applies to international armed conflict. Those rules are, on the whole, more comprehensive than the rules governing the behavior of non-state actors in a non-international armed conflict. (For instance, non-state actors do not need to treat captured government forces as POWs, entitled to the full protections of the Geneva Conventions, though they are bound by the humane-treatment obligations of Common Article 3.)

For a state in this position, working through a non-state actor may seem an appealing alternative. Instead of sending the state’s armed forces into the conflict, the state might instead provide material support to the non-state group fighting on its side of the conflict. Because of the accountability gap left by modern attribution doctrine, the chances that the conduct of the non-

\textsuperscript{98} [CU]
state actor will be attributed to the state are slim. Even the less generous overall control standard allows states to provide significant support to non-state actors without triggering legal responsibility.

States thus have ample incentives to capitalize on modern attribution doctrine by using non-state actors as proxies to accomplish what international law otherwise forbids. As a result, states may hope to act with impunity through their non-state partners in situations where international law bars states from acting themselves. This, in turn, renders some of the most important international legal limits on states deeply vulnerable.

B. The Incentive Not to Exercise Control Over Non-State Actors

There is an additional set of perverse incentives created by the bright-line approach of modern attribution doctrine: States may be reluctant to exercise control over their non-state partners in ways that might minimize the risk that they will violate international law. In fact, states might even be said to have an incentive not to train and instruct non-state partners to comply with international law. Training and instructions might serve as evidence that the state exercised the level of control required to attribute the wrongful conduct of non-state actors to the state. Again, this is true regardless of the specific test applied, whether effective control or overall control.

Consider again a situation in which a state supports a non-state group seeking to overturn its government. In an ideal world, the state would choose to instruct and train the non-state actor to capture rather than kill enemies
who surrender, to refrain from torturing detainees, and to ensure the material and procedural conditions of confinement do not render detention arbitrary—both in order to comply with their Common Article 3 obligations and to avoid mass atrocities and war crimes. However, engaging in such instruction and training might bring the state closer to the strict liability line. In particular, this additional instruction and training—and the level of control required to implement it—could tip the state over the bright line for attribution. The state’s efforts to comply with IHL could even render it responsible for the non-state actor’s *ultra vires* war crimes.

Under existing doctrine, states cannot mitigate responsibility for a non-state actor’s conduct once they have met the requisite threshold of control. Furthermore, any and potentially all actions of the non-state actor—including *ultra vires* actions—may be attributed to a state as if its own agents or organs had performed them. State actors may therefore understandably be concerned that more oversight over non-state actors (even in the form of *ex ante* and *ex post* measures designed to encourage non-state actors’ compliance with the rule of law) will only bring states acting in good faith closer to the attribution line. Once the control threshold has been reached, current doctrine provides states with no explicit mitigation defense that lessens the extent of liability.

Modern attribution doctrine arguably creates precisely the wrong incentives. Where states do work with non-state actors to ensure compliance
with international norms, the law should decrease rather than increase the possibility of attribution of internationally wrongful *ultra vires* acts, encouraging states to take steps to mitigate and avoid violations. Indeed, the common practice of international humanitarian organizations and NGOs—which encourage states partnering with NSAs to train leaders and secure assurances of lawful conduct, among other recommendations—suggests that an accountability regime that opens a state up to liability for exercising due diligence vis-à-vis non-state partners may be counterproductive. In the next two Parts, we consider ways in which these incentives might be significantly mitigated.

III. How to Fill the Gap: Common Article 1 Due Diligence Standard

Thus far this Article has examined modern attribution doctrine in isolation. This has long been the approach to state responsibility. Here we change course. We argue that, in the context of armed conflict, attribution doctrine can only be properly understood in concert with other legal frameworks—in particular, with the legal obligations created by international humanitarian law. Indeed, Common Article 1 of the Geneva Conventions provides a source of state responsibility for the actions of non-state actors that cures many of the deficiencies of state attribution doctrine viewed on its own.99

---

99. The obligations established in Common Article 1 operate in addition to, not in lieu of, the
This is a unique moment to embrace a broader and more integrated understanding of state responsibility doctrine, one that incorporates a robust understanding of Common Article 1. On March 22, 2016, the International Committee for the Red Cross issued its first revised commentaries on the Geneva Conventions in more than six decades. These revised commentaries adopt a broader vision of Common Article 1—a vision that, if embraced by states, could cure many of the infirmities of state responsibility doctrine in the context of armed conflict. In particular, the Commentary of 2016 argues for a more robust reading of Common Article 1’s “to ensure respect” provision. On the ICRC’s view, this clause entails both negative

rules on attribution in the Draft Articles. Article 55 of the Draft Articles provides that a more specific rule on state responsibility may replace general rules on state responsibility codified in the Draft Articles. Draft Articles, supra note 13, art. 55. However, the ILC notes in its commentary that this principle of lex specialis applies only when there is “some actual inconsistency between [the rules].” Id., art. 55, cmt. 4. Since there is no inconsistency between the obligations of Common Article 1 and the rules on attribution in the Draft Articles, both are applicable. Indeed, the I.C.J. in Nicaragua applied both Common Article 1 and the general rules on attribution. See Nicaragua, 1986 I.C.J., ¶¶ 109, 115, 220.


101. Id., art. 1. For the most directly relevant and significant contributions to the literature on “to ensure respect” duties, see generally Fateh Azzam, The Duty of Third States to Implement and
duties “neither to encourage, nor aid or assist in violations of the Conventions” and positive duties that High Contracting parties “must do everything reasonably in their power to prevent and bring such violations to an end.”

This Part of the Article makes the case in three steps: First, it outlines Common Article 1 obligations and explains the case law supporting the extension of the duty to “ensure respect” to states’ interactions with non-state partners. Second, it explains the new 2016 ICRC Commentaries and their decision to embrace an expansive vision of Common Article 1 obligations that include positive due diligence obligation on states working with non-state actors. Third, it explains why Common Article 1, as interpreted in the 2016 Commentaries, promises to close the accountability gap left by modern attribution doctrine and address the perverse incentives described in Part III.


102. ICRC, supra note 11, art. 1, ¶ 154 (2016).
A. Common Article 1 Duties Prior to the 2016 Commentaries

Common Article 1 provides: “The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances.” The ICJ recognized that Common Article 1’s “to ensure respect” provision obligates state parties in both its Nicaragua judgment and Wall advisory opinion. Despite this, Common Article 1 is often forgotten as a source of legal obligation in discussions of state responsibility. However, thanks to recent efforts by the International Committee for the Red Cross advocating a more robust reading of Common Article 1’s “to ensure respect” provision, viewing attribution doctrine in isolation is no longer possible.

A state’s obligations under Common Article 1 are both broader and narrower than its obligations under the Draft Articles. Common Article 1 obligations are broader because states’ duties to “ensure respect” for the rules set forth in the Geneva Conventions are distinct from—and arguably much more extensive than—duties “to respect” the Conventions. But Common


Article 1 obligations are narrower in that they only pertain to violations of parties’ duties under international humanitarian law. By contrast, the Draft Articles address state responsibility for any “internationally wrongful act.” In the context of armed conflict, Common Article 1’s obligation on states “to ensure respect” implies that states have responsibility to make sure their non-state actor partners abide by their IHL obligations, even when the state’s relationship with the non-state actor falls short of standards of attribution under the Draft Articles.

It is widely accepted that compliance with IHL is the responsibility of parties to any international or non-international armed conflict and that Common Article 1 is customary international law. Duties “to respect” IHL

105. In the 2016 commentaries, the ICRC also explicitly adopts the view that non-state parties to an armed conflict are bound by Common Article 3 of the Geneva Conventions. ICRC, supra note 11, art. 1, ¶ 15. Additionally the ICRC argues that non-state actors also incur duties “to ensure respect” for Common Article 3 as it pertains to their members and those acting on their behalf. Id. (“It follows from common Article 3, which is binding on all Parties to a conflict, that non-State armed groups are obliged to ‘respect’ the guarantees contained therein. Furthermore, such groups have to ‘ensure respect’ for common Article 3 by their members and by individuals or groups acting on their behalf. This follows from the requirement for armed groups to be organized and to have a responsible command which must ensure respect for humanitarian law. It is also part of customary international law.”) (citations omitted).

apply directly to states and their organs. The relevant inquiry for determining whether a state is responsible for a non-state actor’s violations of “to respect” duties of Common Article 1 thus concerns the degree to which actors or acts can be seen as attributable to the state. The tests for state responsibility codified in the Draft Articles and articulated in the jurisprudence of the I.C.J. and ICTY also apply to liability for non-state actor violations of “to respect” duties under Common Article 1.

1. The I.C.J.’s “Not to Encourage” Standard

In Nicaragua, the I.C.J. refused to attribute the action of the contras to the United States. But it then went on to consider the applicability of an alternate source of legal obligation—Common Article 1. It determined that the Common Article 1 duty to “ensure respect” also creates an obligation for the state not to assist or “encourage” others (whether states or non-state actors) to violate their obligations under the Geneva Conventions. It explained:

The Court considers that there is an obligation on the United

107. See Crawford, supra note 13, at 43 (providing, as an example, a ruling by the International Court which stated that “[an act] will be considered as attributable to a State if and to the extent that the [the acts] that have been committed by organs or persons other than the State’s own agents were carried out, wholly or in part, on the instructions or directions of the State, or under its effective control”).

States Government, in the terms of Article 1 of the Geneva Conventions, to “respect” the Conventions and even “to ensure respect” for them “in all circumstances”. The United States is thus under an obligation not to encourage persons or groups engaged in the conflict in Nicaragua to act in violation of the provisions of Article 3 common to the four 1949 Geneva Conventions.

The ICJ held that the United States had violated this obligation by publishing and distributing a manual on psychological operations that encouraged the commission of IHL violations. In applying this principle, the ICJ noted that it evaluated whether the “encouragement” in question pertained only to violations of Common Article 3 of the Geneva Conventions, which creates obligations for both non-state actors and state parties to armed conflict. With regard to the handbook, the ICJ found that the United States encouraged the extrajudicial killing of noncombatants in violation of Common Article 3. The ICJ thus explicitly distinguished duties under Common Article 1 not to “incite” or “encourage” violations of Common Article 3 from state responsibility for the actions of the paramilitary

109. Id. (emphasis added).
110. Id. ¶ 256.
111. Id. ¶¶ 255–56.
112. Id. ¶ 256.
groups.\textsuperscript{113} The ruling indicates that the standard for finding responsibility for violating the Common Article 1 duty to “ensure respect” is less stringent than that of state responsibility for attribution of a non-state actor’s acts. This section of the opinion focuses on state “encouragement” rather than state control.\textsuperscript{114} The ICJ found that the United States knew of allegations that the contras were violating IHL and held that knowledge of these allegations was sufficient to show the foreseeability of future IHL violations by the non-state actor.\textsuperscript{115} Significantly, the ICJ found a breach of customary international law

\textsuperscript{113} See id. ¶ 255 (“The question here does not of course relate to the definition of the circumstances in which one State may be regarded as responsible for acts carried out by another State, which probably do not include the possibility of incitement.”).

\textsuperscript{114} Id. ¶ (“[I]t is material to consider whether that encouragement was offered to persons in circumstances where the commission of such acts was likely or foreseeable.

\textsuperscript{115} Id. ¶ 256 (“When considering whether the publication of such a manual, encouraging the commission of acts contrary to general principles of humanitarian law, is unlawful, it is material to consider whether that encouragement was offered to persons in circumstances where the commission of such acts was likely or foreseeable. The Court has however found (paragraph 121) that at the relevant time those responsible for the issue of the manual were aware of, at the least, allegations that the behaviour of the contras in the field was not consistent with humanitarian law; it was in fact even claimed by the CIA that the purpose of the manual was to ‘moderate’ such behaviour. The publication and dissemination of a manual in fact containing the advice quoted above must therefore be regarded as an encouragement, which was likely to be effective, to commit acts contrary to general principles of international humanitarian law reflected in treaties.”).
duties even though the CIA framed the manual as an attempt to moderate the IHL violations of the *contras*.

In its compendium on the “rules of customary international humanitarian law,” the ICRC argues that state practice supports the ICJ’s ruling in *Nicaragua*. According to Rule 144 of the compendium, “States may not encourage violations of international humanitarian law by parties to an armed conflict. They must exert their influence, to the degree possible, to stop violations of international humanitarian law.”\(^{116}\) In commentaries on this rule, the ICRC argues that years of state practice also support a customary international law obligation “not to encourage” violations of IHL. While *Nicaragua* remains the clearest and most compelling articulation of this standard, the ICRC and other scholars make a strong case that state practice, ICTY cases, U.N. resolutions, and U.N. committee reports support its judgment.\(^{117}\)

\(^{116}\) HENCKAERTS & DOSWALD-BECK, supra note 106, at 509 (Rule 144 of customary international humanitarian law).

\(^{117}\) Id. at 512 (“The Trial Chamber of the International Criminal Tribunal for the Former Yugoslavia stated in its judgments . . . that the norms of international humanitarian law were norms *erga omnes* and therefore all States had a ‘legal interest’ in their observance and consequently a legal entitlement to demand their respect. State practice shows an overwhelming use of (i) diplomatic protest and (ii) collective measures through which States exert their influence, to the degree possible, to try and stop violations of international humanitarian law.”). For additional support that Common Article 1 and customary international law require states not to encourage
In sum, under *Nicaragua*, state encouragement of a non-state actor’s actions may be unlawful and trigger state liability under Common Article 1 when it is “likely or foreseeable” that the non-state actor will commit the suggested violations. Even providing advice geared towards moderating a non-state actor’s violations of IHL could render a state responsible for a violation of Common Article 1.\(^{118}\)

2. Positive “Third-State” Obligations

other states and non-state actors to violate IHL, see Azzam, *supra* note 100, at 69 (explaining that the scope of the duty of third states includes a duty not to encourage offending states in further violations); Boisson de Chazournes & Condorelli, *supra* note 100, at 68 (“Some fifty years ago, the drafting of [the Geneva Conventions] led to the inclusion in their common Article 1 of a provision chat provides the nucleus for a system of collective responsibility.”); Kessler, *supra* note 103, at 498 (arguing that states’ duties are more extensive than a cursory interpretation of “ensure respect” might imply).

118. It remains unclear whether states that make a good faith effort to encourage non-state actors to abide by IHL will still be held to violate their Common Article 1 duties. In *Nicaragua* the ICJ found the US liable for violating Common Article 1 because of a CIA manual that the US claimed was intended to discourage the *contras* from violating IHL. 1986 I.C.J., ¶ 255–56. The ICJ took the manual’s recommendations geared towards “mitigating” the violations of the *contras* as evidence that US knew future violations were “likely or foreseeable.” The ICJ, however, also found that the manual included additional recommendations that encouraged violations of IHL. It remains unclear whether future courts will find good faith instructions intended to mitigate non-state actors IHL violations sufficient to violate Common Article 1 duties absent additional “encouragements” to violate IHL.
In its 2004 *Wall* Advisory Opinion, the ICJ adopted an even more generous reading of Common Article 1 than it had in *Nicaragua*. The ICJ found that the Article not only imposed negative duties “not to encourage” abuses, but that the Article also imposed some *positive* third-state obligations. Moreover, unlike negative duties “not to encourage” that are owed to specific actors, the ICJ explained that third state obligations are *erga omnes* obligations owed to the international community as a whole. Such obligations typically have been construed as a general grant of authority for third states to act to ameliorate grave breaches of the Conventions or other *jus cogens* violations (including breaches of the 1949 Genocide Convention). The ICJ interpreted Common Article 1 to imply that “every state party” to the Fourth Geneva Convention had an obligation to “ensure that the requirements” of the Convention are upheld: “[E]very State party to that Convention, whether or not it is a party to a specific conflict, is under an obligation to ensure that the requirements of the instruments in question are

119. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 131 (July 9) [hereinafter *Wall* Advisory Opinion].

120. *Id.* ¶ 156–60.

121. *Id.* ¶ 157. [EN7]

122. See CHRISTIAN J. TAMS, ENFORCING OBLIGATIONS ERGA OMNES IN INTERNATIONAL LAW 139–40 (2010).

complied with."  

In its application of this principle, the ICJ held that “all the States parties to the Geneva Convention . . . are under an obligation, while respecting the United Nations Charter and international law, to ensure compliance by Israel with international humanitarian law as embodied in that Convention.”  

The ICJ thus explicitly found that Common Article 1 imposed third-state obligations on all High Contracting Parties to halt Israel’s violation of the Fourth Convention. Given that many state parties do not have direct ties to Israel’s military action in Palestine, the ICJ opinion implies that this duty exists regardless of whether a state had provided support to Israel or “encouraged” its violations.

In a separate opinion, Judge Kooijmans clarified that he disagreed with the majority precisely because it interprets Common Article 1 as entailing positive duties:

    I simply do not know whether the scope given by the Court to [Common Article 1] in the present Opinion is correct as a statement of positive law. . . . I fail to see what kind of positive action, resulting from this obligation, may be expected from individual States, apart from diplomatic démarches.


125.  *Id.* ¶ 159.

126.  *Id.* ¶ 50 (separate opinion by Kooijmans, J.) (emphasis added).
The separate opinion helps elucidate two points: first, that the ruling does impose some positive third-party obligations on states; and second, that the scope of these obligations remains under-specified.

ICJ case law on Common Article 1 thus supports the conclusion that Common Article 1 imposes not only negative duties “not to encourage” violations of international humanitarian law, but also some minimal positive third-state obligations. Considering the Nicaragua and Wall cases together, it may be that Nicaragua indicates the “floor” or minimal conditions that would suffice to establish a violation of the Common Article 1 duties “to ensure respect.” The Wall Advisory Opinion takes this a step further, suggesting that third states might even be liable for their failure to take preventative action against foreseeable IHL violations by other states.\textsuperscript{127}

B. \textit{The 2016 ICRC Commentaries: Embracing a Positive Due Diligence Obligation}

On March 22, 2016, the ICRC released the first major new Commentaries on the Geneva Conventions since the famous 1952 Pictet Commentaries.\textsuperscript{128} The release followed several years of preparations. In the

\textsuperscript{127} See supra notes 124–126.

period preceding the release, the legal staff of the ICRC published interpretations of the legal obligations under Common Article 1 under their own names, providing a preview of the Commentaries to come. These initial releases provoked controversy and push-back by states, which caused the release to be delayed by more than half a year. The final release promises to be a signal moment in the development of international humanitarian law—and an important touchstone for understanding of legal obligations of states under the Geneva Conventions for decades to come.

Building on Nicaragua and Wall, the ICRC legal staff argued in its pre-commentary writings that duties “to ensure respect” should include “positive” third-state obligations to prevent and halt other states’ and non-state actors violations of the Conventions. This proposed expansion suggests only that states are required to take “all possible steps, as well as any lawful means at their disposal” to “ensure” all other parties to armed conflict respect the Geneva Conventions. In contrasting its interpretation of Common Article 1 with a narrower view, the ICRC’s Commentary of 2016 also makes clear that states’ duties to ensure respect extend to their

129. Dörmann & Serralvo, supra note 100.


132. Id. at 724.
interactions with both states and non-state actors.\textsuperscript{133}

Additionally, the ICRC legal staff and Commentary of 2016 argue that a “due diligence” standard should apply when determining whether states have discharged positive “to ensure respect” obligations.\textsuperscript{134} This standard

\begin{quote}
133. ICRC, \textit{supra} note 11, art. 1, ¶ 120 (2016). (“The interpretation of common Article 1, and in particular the expression ‘ensure respect’, has raised a variety of questions over the last decades. In general, two approaches have been taken. One approach advocates that under Article 1 States have undertaken to adopt all measures necessary to ensure respect for the Conventions only by their organs and private individuals within their own jurisdictions. The other, reflecting the prevailing view today and supported by the ICRC, is that Article 1 requires in addition that States ensure respect for the Conventions by other States and non-State Parties.”).

134. Dörmann & Serralvo, \textit{supra} note 100, at 722–25; ICRC, \textit{supra} note 11, art. 1, ¶ 165 (2016). Due diligence is not a novel standard; international courts and commentators have relied on similar standards under various international human rights frameworks. The Inter-American Court and the European Court of Human Rights have interpreted similar “to ensure respect clauses” in their respective human rights treaties as imposing positive due diligence obligations on states. See \textit{infra} note 146. Commentators have also argued states and corporations have positive due diligence obligations in the context of corporate social responsibility. The Guiding Principles on Business and Human Rights provide that positive obligations include, but are not limited to “human rights due diligence,” which requires business enterprises “to identify, prevent, mitigate and . . . [assess responses to] adverse human rights impacts.” U.N. \textsc{Human Rights Office of the High Comm’r, U.N. Guiding Principles on Business and Human Rights}, Principle 17, U.N. Sales No. HR/PUB/11/04 (2011). The Guiding Principles also provide that states should take steps to prevent human rights abuses by enterprises that are owned or controlled by the state, “or that receive substantial support and services from State agencies.” \textit{Id.} Principle 4. Interestingly, in the context of corporate social responsibility, some corporate counsel have raised concerns that exercising due
\end{quote}
would impose obligations on the conduct of states, but does not require them to attain specific outcomes. 135 States are not to be held responsible for failures to prevent other states from violating the Conventions as long as they can show that they "made every effort" 136 to prevent the violation. 137 The diligence could increase exposure to liability by making the company aware of potential risks, imposing positive duties to mitigate. These concerns are not unlike some of the objections that detractors of a more expansive reading of Common Article 1 might raise. In the context of corporate social responsibility, the short response seems to be that these concerns are overstated. Due diligence allows companies to "identify potential human rights risks and address them before they occur, which should reduce a company’s exposure to litigation of all kinds, and help the company defend against human rights claims that might be filed." John F. Sherman, III & Amy Lehr, Human Rights Due Diligence: Too Risky? 4 (Corporate Social Responsibility Initiative, Working Paper No. 165, 2010).

135. Dörmann & Serralvo, supra note 101, at 723–25; see also ICRC, supra note 11, art. 1, ¶ 65 (2016). [Matt EN: unclear whether this should be 65 or 165 – please double check].


137. ICRC legal commentators have been clear, however, that general prohibition on the use of force of Article 2(4) of the U.N. Charter provides the upper limit on actions states may take to discharge their Common Article 1 obligations. Third state obligations under Common Article 1 could not to be used as a means to justify unilateral humanitarian interventions. See Dörmann & Serralvo, supra note 101, at 725–26. ("CA 1 should not be used to justify a so-called ‘droit d’ingérence humanitaire.’ In principle, permitted measures must be limited to ‘protest, criticism, retorsions or even non-military reprisals.’). Armed intervention may only be decided within the context of the UN, and in full respect of the UN Charter. The rules on the resort to armed force (jus ad bellum) govern the legality of any use of force, even if it is meant to end serious violations of
ICRC publications foreshadowed the new commentaries on the Geneva Conventions that also embrace these positive obligations of third states to "ensure respect" of the Conventions by other states and non-state actors.\textsuperscript{138}

Importantly, the ICRC embraces an interpretation of Common Article 1 obligations that, unlike attribution doctrine, does not establish a bright-line rule. Indeed, the Commentary of 2016 makes it clear that duties to ensure respect extend to state interactions with private persons, even when such persons' conduct is "not attributable to the state."\textsuperscript{139} Instead, there is a

IHL. The content of CA 1 is not part of jus ad bellum and thus cannot serve as a legal basis for the use of force."). For an extended and speculative discussion of possible options a state may take to discharge "to ensure" Common Article 1 duties, see Umesh Palwankar, Measures Available to States for Fulfilling their Obligation to Ensure Respect for International Humanitarian Law, 33 INT’L REV. RED CROSS 1, 925 (1993).

138. For the most directly relevant and significant contributions to the literature on "to ensure respect" duties, see Fatch Azzam, The Duty of Third States to Implement and Enforce International Humanitarian Law, 66 NORDIC J. INT’L L. 55, 57 (1997); Boisson de Chazournes & Condorelli, supra note 101; Carlo Focarelli, Common Article 1 of the 1949 Geneva Conventions: A Soap Bubble, 21 EUR. J. INT’L L. 125, 138 (2010); Frits Kalshoven, The Undertaking to Respect and Ensure Respect in All Circumstances: From Tiny Seed to Ripening Fruit, 2 Y.B. INT’L HUMANITARIAN L. 3, 31 (1999).

139. ICRC, supra note 11, art. 1, ¶ 150 (2016). (“The duty to ensure respect covers not only the armed forces and other persons or groups acting on behalf of the High Contracting Parties but extends to the whole of the population over which they exercise authority, i.e. also to private persons whose conduct is not attributable to the State. This constitutes a general duty of due diligence to prevent and repress breaches of the Conventions by private persons over which a State exercises
sliding scale that adjusts state legal obligations based on their degree of connection and control. The Commentary of 2016 makes clear that duties to ensure respect extend to any efforts to finance, equip, arm or train the armed forces of parties to a conflict. Prior to the release of the commentaries, the ICRC legal staff additionally characterized “third state” duties as context-dependent obligations, which increase in scope according to a state’s engagement with a party to a conflict. Accordingly, significant ties (whether diplomatic, geographic, social, or economic) between states increase the due diligence responsibility that arises vis-à-vis other states and non-state actors under the Common Article 1 obligation to ensure respect for the Conventions.

Even in the new commentaries, however, it is unclear whether and how

authority . . .” (citations omitted).

140. Id. art. 1, ¶ 167 (“The duty to ensure respect for the Geneva Conventions is particularly strong in the case of a partner in a joint operation, even more so as this case is closely related to the negative duty neither to encourage nor to aid or assist in violations of the Conventions. The fact, for example, that a High Contracting Party participates in the financing, equipping, arming or training of the armed forces of a Party to a conflict, or even plans, carries out and debriefs operations jointly with such forces, places it in a unique position to influence the behaviour of those forces, and thus to ensure respect for the Conventions.”)

141. Id.


143. Id. at 725.
obligations based on “context” are derived from the third-party state’s capacity for influence in a given situation. On one reading, a state might incur greater Common Article 1 obligations in any given conflict simply by virtue of its pervasive worldwide military, economic, and diplomatic influence.\textsuperscript{144} In alternative construction, a state might be required to take voluntary steps to engage another state or non-state actor in order to comply with its Common Article 1 due diligence obligations. At the very least, direct support for another state’s involvement in an armed conflict would increase a third state’s responsibility under Common Article 1. The lack of clarity on the scope of the obligation has been part of the reason states have been slow to embrace the new Commentaries on this point.

C. \textit{Closing the Gap}

The Commentary of 2016 supports a reading of Common Article 1 as entailing positive obligations for states regarding the conduct of non-state actors. There is good reason to embrace this reading. First, the text, commentary, and case law support it. Second, applying due diligence obligations to states working with non-state actors would close much of the accountability gap otherwise left by state responsibility doctrine.

The text of Common Article 1 itself offers no basis for distinguishing

\footnote{144. \textit{Id.} at 724.}
between state actors and non-state actors.\textsuperscript{145} The Article simply provides that “[t]he High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances.”\textsuperscript{146} This entails duties to ensure respect by other State Parties. But non-state actors also have both legal rights and legal responsibilities under Common Article 3. Hence, the best reading of Common Article 1 is that offered by the ICRC: the duty to “ensure respect” ought to be read to require states to ensure respect by state and non-state actors engaged in armed conflict.

Existing case law supports this reading of Common Article 1. The ICJ in \textit{Nicaragua} concluded that states have some Common Article 1 duties toward non-state actors.\textsuperscript{147} This reading finds support, moreover, in related

\textsuperscript{145} For the idea that third state obligations apply to states and non-state parties alike, see Dieter Fleck, \textit{International Accountability for Violations of the Ius in Bello: The Impact of the ICRC Study on Customary International Humanitarian Law}, 11 J. CONFLICT & SECURITY L. 179, 182 (2006) (“[The obligation to ensure respect] extends to acts of third states, not directly involved in an armed conflict, in their relations to state and non-state parties to the conflict.”). See also Hannah Tonkin, Common Article I: A Minimum Yardstick for Regulating Private Military and Security Companies, 22 LEIDEN J. INT’L L. 779, 783 (2009) (“According to the ICRC, [the obligation to ensure respect] imposes a legal obligation not only on the parties to the armed conflict, but also on third states not involved in the conflict.”).

\textsuperscript{146} Geneva Convention I, supra note 10, at 3116.

\textsuperscript{147} \textit{Nicaragua}, 1986 I.C.J., ¶ 220 (“The Court considers that there is an obligation on the Government, in the terms of Article 1 of the Geneva Conventions, to “respect” the Conventions and even “to ensure respect” for them “in all circumstances[,]”).
case law by the European Court of Human Rights and the Inter-American Court of Human Rights. Both have interpreted their respective conventions, which contain similar duty to “ensure” language, to impose affirmative “due diligence” obligations on State Parties for the conduct of non-state actors within their territory. 148

Commentators have similarly argued that there are “due diligence” obligations under Common Article 1, 149 in particular with regard to the use of private military and security contractors by states. 150 Additionally, other scholars have suggested affirmative due diligence obligations extend to the context of U.S. support for paramilitary groups in Syria. 151 Hannah Tonkin argues that a state’s due diligence obligations towards the conduct of private


150. Hannah Tonkin, State Control Over Private Military and Security Companies in Armed Conflict 136 (2011) (“If the host state does not take adequate measures to control a PMSC and the company violates IHL in state territory, the state could incur international responsibility for its failure to ensure respect for IHL. Although no court to date has found a state responsible under Common Article 1 merely on the basis of such inaction, the above analysis has shown that this pathway to responsibility is certainly possible in principle.”).

military and security contractors will vary with context. In her analysis, three factors are relevant for determining a state’s due diligence requirements: the level of control a state exercises over the non-state actor, the risk the non-state actor will violate IHL, and the state’s actual or constructive knowledge of this risk. Arguably, a state dealing with a non-state actor will need to take additional measures to ensure compliance with IHL when any one of these factors is present to a significant degree.

Applying the ICRC reading of the “to ensure respect” provision of Common Article 1 significantly ameliorates the gap in current state responsibility doctrine. Unlike the attribution framework of the Draft Articles, Common Article 1 creates obligations for states to ensure compliance even when they do not exercise effective or overall control over a non-state actor. As *erga omnes* obligations, states owe Common Article 1 duties not only to the particular parties to an armed conflict but also towards the international community as a whole. Moreover, Common Article 1’s


153. *Id.* at 794 (“Just as the measures necessary to discharge the due diligence obligation may vary between states, so too may the measures required of a particular state vary with the circumstances. Three factors are particularly pertinent to this assessment: first, the level of influence or control that the hiring state in fact exercises over the PMSC in question; second, the risk that the company’s activities will give rise to a violation of IHL; and third, the state’s actual or constructive knowledge of that risk.”).

154. ICRC, *supra* note 11, art. 1, ¶ 119 (“Moreover, the proper functioning of the system of
text stipulates that the High Contracting Parties must ensure respect for the Conventions “in all circumstances.”\(^{155}\) As a result, these obligations do not have a geographic or temporal threshold: Common Article 1 duties apply to any and all state interactions with a non-state actor whenever the Geneva Conventions are applicable.

A breach of Common Article 1 duties differs from a finding of attribution liability. The Commentaries of 2016 rightly characterize Common Article 1 duties and state responsibility doctrine as “operat[ing] at different levels.”\(^{156}\) States failing to discharge their duties to ensure respect by partner non-state actors would be found responsible for violating their own international legal obligations. Instead of imputing the actions of the non-state actor to the state, then, Common Article 1 creates a direct duty on the

---

\(^{155}\) Id. ¶ 145 (“The novelty of the provision lies in the addition of the duty to ‘ensure respect’, which must be done ‘in all circumstances’. This sets a clear standard, as ‘ensuring’ means ‘to make certain that something will occur or be so’ or inversely ‘make sure that (a problem) does not occur’. States are thus required to take appropriate measures to prevent violations from happening in the first place. Accordingly, the High Contracting Parties must—starting in peacetime—take all measures necessary to ensure respect for the Conventions.”).

\(^{156}\) Id. at ¶ 160.
part of a state to ensure respect by non-state actors. For example, when a state’s non-state partner commits war crimes in violation of its Common Article 3 obligations, a state would be held responsible for breach of its Common Article 1 duties, not for the war crimes themselves. To take a simple analogy, the difference between attribution doctrine and Common Article 1 is akin to the difference between holding a company responsible for the actions of an employee because those actions can be attributed, or imputed, to the company and holding a company responsible for failing to take steps to prevent its employees from taking certain actions.

Because Common Article 1 places direct duties on states, it establishes “more stringent conditions than those required for the secondary rules on State responsibility for aiding or assisting.” State support that facilitates non-state groups’ ability to commit violations of international humanitarian law constitutes an independent violation of the state’s Common Article 1 duties, even if such actions may not pass the attribution bar under state responsibility doctrine.\textsuperscript{158}

\textsuperscript{157} Id. ("Common Article 1 and the rules on State responsibility thus operate at different levels. The obligation to ensure respect for the Conventions is an autonomous primary obligation that imposes more stringent conditions than those required for the secondary rules on State responsibility for aiding or assisting.").

\textsuperscript{158} Id. ("Financial, material or other support in the knowledge that such support will be used to commit violations of humanitarian law would therefore violate common Article 1, even though it may not amount to aiding or assisting in the commission of a wrongful act by the receiving States\).
This broad application of Common Article 1 duties would require states to make respect of international law a major focus of their interactions with non-state actors in armed conflicts. In fulfilling their Common Article 1 to “ensure respect” obligations, states would be required to take affirmative steps to ensure their non-state partners complied with relevant law. Failures to properly instruct and train non-state partners in their international law obligations could thus be construed as a violation of a state’s Common Article 1 duties.

Under the proposed framework of the 2016 Commentaries, states have obligations to take significant action towards insuring international law compliance in at least two ways. First, following Nicaragua, states must adequately assess whether assisting a non-state actor is likely or foreseeable to lead to violations of the Geneva Conventions; if a state’s assistance to a non-state actor will enable violations of the Conventions, Common Article 1 requires that they forgo offering such assistance.159 Second, when states do engage in partnerships with non-state actors in armed conflicts, Common Article 1 requires that, even in relatively low-level engagements (supplying equipment, providing arms, or sharing intelligence), states must exercise due diligence and take affirmative steps to ensure the non-state actors comply

for the purposes of State responsibility.”).  

159. See supra Part III.A.1 for a discussion of a state’s responsibility not to encourage or assist a non-state actor in the commission of acts that violate IHL.
with the Geneva Conventions.\textsuperscript{160}

Common Article 1 has the potential to eliminate the perverse incentive for states to avoid fully engaging with non-state partners as a means of skirting responsibility for violations of the laws of armed conflict: the very failure to ensure non-state actor compliance with international law could—even absent a finding of state control—still be the basis of state liability. Moreover, any deliberate effort to use a non-state actor to engage in conduct that violates the Conventions would clearly violate Common Article 1. Common Article 1 duties thus encourage states to make compliance with the Geneva Conventions a central feature of their broader foreign policy agendas.

In sum, Common Article 1, as interpreted by the ICRC in its new Commentaries, promises to close much of the state responsibility gap identified in Part III. Common Article 1 requires states to exercise due diligence to ensure that their non-state actor partners respect international law, even if the level of control they exercise falls short of what would be necessary to trigger modern attribution doctrine. These Common Article 1 duties are not only important as a set of stand-alone obligations. They help alleviate the perverse incentives that can otherwise be created by modern attribution doctrine’s bright line rule.

\textsuperscript{160} See \textit{infra} Part VI for a discussion of steps we recommend states take to discharge these duties.
IV. Getting the Incentives Right: An Affirmative Defense

There is just one problem: States seeking to comply with their Common Article 1 duties might fear triggering liability under attribution doctrine. While Common Article 1 duties may be discharged under a due diligence framework—in which adequate effort to discharge a duty would shield a state from liability—overall control and potentially effective control function as a regime of strict liability under which even ultra vires acts may be attributed.\(^{161}\) In other words, a state seeking to meet its due diligence obligations under the ICRC’s reading of Common Article 1 might trip over the bright line drawn by attribution doctrine.

As a result, even states that do not intend to use non-state actors to skirt their international responsibilities may be reticent to embrace a reading of Common Article 1 that imposes positive due diligence obligations to curb potential violations of IHL by non-state partners. States are likely to be concerned that measures taken to discharge Common Article 1 obligations may contribute to breaching the attribution threshold. Under the strict and overall control standards, once the state meets the requisite level of control, all of the conduct of non-state actors—including ultra vires actions—can be imputed to the state regardless of the kinds of measures the state took to

\(^{161}\) For a discussion of liability for ultra vires action under effective control, see supra notes 46–55 and accompanying text.
prevent violations. Under the effective control standard, at least some of the *ultra vires* conduct of non-state partners may be imputed to the state. The ILC has clarified that under Article 8, a state may be held responsible for *ultra vires* acts during operations over which a state exercises “effective control,” as long as those acts are “an integral part” of the operation.\textsuperscript{162} However, it does not extend responsibility to *ultra vires* acts that are only “incidentally or peripherally” associated with an operation.\textsuperscript{163} This example illustrates yet again how the strict liability regime of attribution doctrine can create incentives for states *not* to provide IHL training and instructions to non-state actors.

The perverse incentives for good faith actors become particularly apparent when we consider the types of factors that courts and commentators examine to establish attribution: support, training, instructions, and strategic guidance. All four overlap with the kinds of activities states are expected to use to discharge their Common Article 1 due diligence duties when they partner with non-state armed groups. This raises the distinct possibility that measures taken by a state to encourage non-state actors to comply with IHL will render the state responsible for any violations non-state actors commit in the course of an operation. This potential for liability means states are likely

\textsuperscript{162} Draft Articles, *supra* note 13, art. 8, cmt. 3.

\textsuperscript{163} Id.
to oppose a reading of Common Article 1 that risks making them responsible for the *ultra vires* actions of non-state groups without any possibility of mitigation.

To address this problem, states ought to be permitted to offer an affirmative defense in cases where actions taken to address Common Article 1 due diligence obligations push them over the bright line for state attribution. Practically speaking, states should be able to invoke such a defense if they are ever brought before an international or domestic court, a human rights body, a special rapporteur, or even if their conduct is simply being assessed by the court of public opinion. The concern is that key evidence of control over a non-state actor could rely on measures taken by a state to prevent violations of IHL by the non-state actor. In a case where a state has taken measures to avoid certain IHL violations by the non-state actor, the state should not be held legally responsible for those *ultra vires* violations. Here we explain how such a legal innovation would work.

A. *An Affirmative Defense to Liability for Ultra Vires Actions*

In order to resolve the perverse incentive problem, we propose an affirmative defense to state liability. In particular, measures taken to fulfill Common Article 1 obligations (hereinafter “Common Article 1 measures”) may be offered as an *affirmative defense* when determining whether *ultra vires* conduct is attributable to the State, or whether under the effective control or overall control standard. States would have less disincentive to
embrace positive obligations under Common Article 1 and to take action to encourage non-state actors to comply with their IHL obligations (for example, offering IHL training to non-state actors).

We are not proposing a change to the law on state responsibility. Instead of modifying the legal standard of effective control, international courts would recognize an affirmative defense in line with the spirit of the current attribution framework. This has the advantage of leaving the attribution framework intact, but allows states to embrace the positive obligations under Common Article 1 without thereby triggering liability for *ultra vires* actions under attribution doctrine.

A comparison to domestic law in the context of Title VII vicarious liability for supervisor harassment offers insight into how this would work.\footnote{164} In *Burlington Industries v. Ellerth*\footnote{165} and *Faragher v. City of Boca Raton*,\footnote{166} the Supreme Court found that employers could be subject to vicarious liability under Title VII to a harassed employee for actionable discrimination caused by a supervisor.\footnote{167} In *Ellerth*, however, the Court allowed employers

---

\footnote{164. We are only offering a loose analogy to illustrate our argument; vicarious liability in the context of domestic employment obviously features a number of elements that differ widely from the context of accountability non-state actor conduct in the context of armed conflict.}

\footnote{165. 524 U.S. 742 (1998).}

\footnote{166. 524 U.S. 775 (1998).}

\footnote{167. See *Ellerth*, 524 U.S. at 765 (holding that an employer is subject to vicarious liability to a}
to raise an affirmative defense to vicarious liability. The defense requires two necessary elements: (1) that "the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior," and (2) that "the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise." The first prong of the Ellerth test is directly analogous to the state responsibility context: States that can show they adequately exercised reasonable care to prevent and correct non-state actor violations of the Geneva Conventions should be able to avoid liability for some non-state actor ultra vires actions.

Adopting this affirmative defense strikes the right balance between accountability and states' concerns about liability risk from positive Common Article 1 obligations. The affirmative defense would only allow states to avoid liability for a narrow set of actions committed by non-state actors: ultra vires actions that violate IHL and are taken against states' efforts to ensure non-state actor compliance with international law. Because it is framed as an affirmative defense, the burden would fall on states to prove that they had adequately discharged their Common Article 1 duties in an effort to avoid the violations. The test thus parallels the domestic example victimized employee for an actionable hostile environment created by a supervisor; Faragher, 524 U.S. at 807 (same).

168. Ellerth, 524 U.S. at 745.
above: a defense to employer liability for supervisory actions requires employers to take adequate steps to ensure supervisors were aware of what actions would constitute harassment.

Moreover, when a state is found to exercise control over a non-state group, the state would not be able to use the affirmative defense to escape liability for the group’s violations of IHL if the state (1) directly instructed the group to commit the violations, or (2) failed to take reasonable steps to insure against the violations. Thus, even with the option of raising an affirmative defense, states could still be held liable for some ultra vires actions taken by a non-state actor. Additionally, as discussed in detail below, the affirmative defense would ameliorate states’ concern about liability for actions done against their instructions—even when a state exercises effective or overall control over a non-state group, proper discharge of its Common Article 1 duties offers a shield against ultra vires liability. Ultimately, this affirmative defense would encourage states to freely sponsor and implement such IHL training programs, without any fear that such programs would be used against them when trying to establish attribution.169

169. It is important to note that in the ICJ’s Bosnian Genocide, the court appears to suggest that ultra vires actions may not be attributable to states under the effective control test. This, however, is an evidentiary issue: the opinion implies that only evidence of direct instructions from the officers of a state to the non-state actor in the prelude to an internationally wrongful act will suffice as the basis for attribution. The effect of this evidentiary rule, however, is to effectively foreclose the
How would this play out in practice? Consider again the not-so-hypothetical case, described above, in which a state supports a non-state group seeking to overthrow its government. Imagine that the state engages in a substantial training program intended to ensure that the members of the non-state group not engage in IHL violations. The training program brings all members of the non-state group together to a camp run by the state’s armed forces. There, the state’s armed forces integrate IHL into their training in ways that are meaningfully intended to inform the non-state actors about international humanitarian law. They also require members of the non-state group that seeks to receive the state’s support to sign declarations in which they commit to abide by IHL (declarations that are meaningfully calculated to be understood by those signing them—written in their own language and read out loud to those who are illiterate). To take these actions, the state will have provided extra financing to the armed group (by financing the training

possibility of a finding of attribution for an ultra vires act. Only acts for which there is evidence the state ordered them are potentially ripe for attribution. An affirmative defense would be unnecessary in this context. The Commentary to the Articles on State Responsibility, on the other hand, leaves open the possibility of attribution of ultra vires acts to the state under effective control. It is difficult to weigh the relative authority of the ICJ and the ILC against each other, with the result that one could plausibly apply either articulation of the standard. The applicability of the affirmative defense, however, avoids the question of relative authority entirely: states can offer the affirmative defense of discharging Common Article 1 duties even if a court had made a determination that effective control already existed.
program) and exercised more managerial control over the non-state actor (by bringing all members of the group to one location and running the program). Moreover, the state will probably also have given more specific directions to the non-state actor (e.g., “Do not attack this village because there are too many innocent civilians.”).

After this training program, imagine that the non-state actor still commits *ultra vires* IHL violations, and an international court, rapporteur, investigative body, or other authority must decide whether the *ultra vires* conduct of the non-state actor is attributable to the state. In this case, the applicable legal standard for state attribution would apply—overall control or effective control. However, if the state could offer a good faith demonstration that the training program was undertaken to discharge its Common Article 1 duties, it could argue that this provides an affirmative defense to attribution of the *ultra vires* conduct—particularly where the training program constitutes a significant source of the evidence that the state exercises the level of control required to trigger attribution.

B. A Solution for Good Faith Actors

The affirmative defense is an ideal solution for “good faith actors” (i.e., states that engage with non-state actors for reasons beyond just trying to avoid responsibility). The affirmative defense would allow them to take reasonable steps to ensure that armed non-state groups with whom they work abide by their IHL obligations. Because any good faith measure they take to
fulfill their Common Article 1 obligations would support an affirmative
defense against attribution of *ultra vires* actions, they would have less reason
for concern that taking such measures would push them across the attribution
threshold.

Not only would the affirmative defense encourage states to fulfill their
Common Article 1 obligations, but it would also encourage states to
recognize the applicability of the Common Article 1 obligation “to ensure
respect” to their relationships with non-state actors. One of the reasons States
may resist the ICRC interpretation of the positive obligation “to ensure
respect” is a fear that taking action to satisfy these obligations could trigger
additional responsibilities. Since the affirmative defense would ameliorate
this problem, it would reduce states’ objections to the ICRC interpretation on
this ground. The net consequence is that there would be greater recognition
of and compliance with the “to ensure respect” obligation under Common
Article 1.

C. *A Solution for Bad Faith Actors*

The affirmative defense does not close the accountability gap that under
existing state responsibility doctrine advantages what we could call “bad faith
actors”: states that deliberately use non-state actors to commit acts they
themselves could not legally do, in order to evade legal responsibility.
Because of the high substantive and evidentiary bars for a finding of
attribution under the effective and overall control standards, bad faith actors
can provide significant support to a non-state actor engaged in internationally wrongful acts without triggering a finding of attribution. These states would, however, be liable for violating their Common Article 1 duties to ensure respect for the Geneva Conventions.

According to the ICRC, the duty to ensure respect under Common Article 1 also imposes due diligence obligations on states to prevent violations of IHL.\textsuperscript{170} This interpretation of Common Article 1 may provide even bad faith actors with an incentive to take prophylactic measures with their non-state proxies, since a state that fails to take measures to avoid violations of law by its proxies will have failed to meet its due diligence obligations. Liability for the failure to uphold Common Article 1 obligations may not be a moral equivalent to a finding of state responsibility where a state has used proxies to evade international law deliberately. However, it can go a significant way toward providing accountability for states that fail to take reasonable measures to prevent international humanitarian law violations and thus, toward creating the proper incentives for states.

V. Recommendations to States in an Era of Uncertainty

The legal landscape we have outlined in this Article is one in which the law of state responsibility remains in flux. There is limited case law on the doctrine of state responsibility, and there is even less on the legal obligations

\textsuperscript{170} ICRC, \textit{supra} note 11, art. 1, \textit{§§} 164–73.
that attend to states under Common Article 1. Nonetheless, the danger for states is a real one: States working with non-state actors must be concerned about legal liability for those non-state actors’ behavior.

Here we propose concrete, IHL-protective measures that states can take to alleviate this danger. These measures would fulfill states’ Common Article 1 duty to ensure respect. Moreover, even absent an affirmative defense for purposes of a finding of attribution, as we recommend in Part IV, the attribution bar is high enough that these measures, taken alone, are unlikely to trigger attribution. These measures also have the important feature of decreasing the likelihood of significant international humanitarian law violations. That should be reason enough for states to take the steps recommended here.

The literature on Common Article 1 does not provide a clear list of what measures a state can take with regard to non-state actors to discharge its Common Article 1 obligations.\textsuperscript{171} However, a number of international NGOs

\textsuperscript{171} Writings by ICRC legal staff have suggested, however, that under Common Article 1 third state obligations are not obligations “of result.” Accordingly, the ICRC argues that due diligence imposes obligations on the conduct of states, but does not require them to attain specific outcomes. States will not be held responsible for failures to prevent other states from violating the Conventions as long as they can show that they “made every effort” to prevent the violation. Dörrmann & Serralvo, supra note 101, at 724. (“[T]he obligation of result is an obligation to ‘succeed’, while the obligation of diligent conduct is an obligation to ‘make every effort’ . . . [T]hird States can only be under an obligation to exercise due diligence in choosing appropriate measures to induce
that engage with non-state actors, such as the ICRC and the humanitarian organization Geneva Call, have recorded best practices for encouraging these actors to respect IHL.\(^{172}\) Drawing on their work, as well as recent regulatory and policy developments in the parallel area of promoting IHL among private military security contractors (PMSCs),\(^{173}\) this Article sets forth some actions belligerents to comply with the law. This does not turn the duty to ensure respect into a vacuous norm, since States are under the obligation, depending on the influence they may exert, to take all possible steps, as well as any lawful means at their disposal, to safeguard respect for IHL rules by all other States. If they fail to do so, they might incur international responsibility.\(^{174}\).

\(^{172}\) See supra notes 169, 174 and accompanying text.

\(^{173}\) Many commentators have elaborated on the positive obligations states have under international law with respect to PMSCs. See, e.g., Lindsey Cameron & Vincent Chetail, Privatizing War: Private Military and Security Companies Under Public International Law 579 (2013) (supporting legislation that would allow exercise of criminal jurisdiction over PMSC employees, as well as regulatory and contractual requirements that PMSCs report serious incidents); Laura A. Dickinson, Contract as a Tool for Regulating Private Military Companies, in From Mercenaries to Market: The Rise and Regulation of Private Military Companies 223–25 (Simon Chesterman & Chia Lehnardt eds., 2007) (suggesting new contractual provisions to agreements between hiring states and PMSCs that would enhance oversight of and compliance by PMSCs with international humanitarian law); Moyakine, supra note 78, at 303–92 (discussing the responsibility of states for non-compliance by PMSCs with international humanitarian law); Expert Meeting on Private Military Security Contractors: Status and State Responsibility for Their Actions, U. CENT. FOR INT’L. HUMANITARIAN L. 34–35 (2005), http://www.geneva-academy.ch/docs/expert-meetings/2005/rapport_compagnies_privees.pdf [https://perma.cc/6679-QT7Z] (discussing whether due diligence obligations to a PMSC applies to the state that hires the PMSC, the state in which the PMSC is conducting operations, or the state in
that a state should (and perhaps must) take with respect to a non-state actor in order to discharge its duties to "ensure respect." These steps are divided into those taken *ex ante* and *ex post*. This is not meant as an exhaustive list of steps states may take to meet their obligations under Common Article 1 when working with non-state actors, but it is meant to be instructive.

Some scholars have argued that the knowledge factor for assessing due diligence requirements under Common Article 1 is more exacting than that under the Draft Articles.¹⁷⁴ In exercising due diligence, states may be held

---

¹⁷⁴ See Dörmann & Serralvo, *supra* note 100, at 734 (under Articles 6 and 7, respectively, of the 2013 U.N. Arms Trade Treaty, a state may not transfer arms to non-state actors if it has
responsible not only if they were “aware” of the risk of a non-state actor’s violation of IHL, but also if they “ought to have been aware” of the likelihood of such violations. In light of this consideration, policies adopted by states to ensure IHL compliance should be established and made clear to all actors in advance, and a non-state actor’s acceptance and understanding of a state’s IHL policies should be a condition precedent to engagement.

knowledge that the recipients will use the weapons to violate the Geneva Conventions or if there is an “overriding risk” of a violation; Tonkin, supra note 144, at 794–95 (a hiring state could be liable for an IHL violation if, in hiring a PMSC, it knows or should know of an increased risk that the PMSC will violate IHL).

175. Tonkin, supra note 145, at 795 (“The third key consideration is whether the hiring state was aware, or ought to have been aware, of the enhanced risk of violation by the PMSC. Although the law of state responsibility contains no general requirement of fault, obligations of prevention frequently require some degree of knowledge or constructive knowledge on the part of the state in order to establish breach. For example, in assessing responsibility for a failure to protect life, the European Court of Human Rights employs a test of ‘foreseeability of the event’: the state is responsible if the authorities knew or ought to have known of the risk to life and failed to take measures which, judged reasonably, might have prevented the occurrence of the fatal event. In similar vein, in the Genocide case the ICJ held that the obligation to prevent and punish genocide applies wherever a state is aware, or should normally be aware, of a serious risk that genocide will occur.”).

176. See Olivier Bangerter, The ICRC and Non-State Armed Groups, in EXPLORING CRITERIA & CONDITIONS FOR ENGAGING ARMED NON-STATE ACTORS TO RESPECT HUMANITARIAN LAW & HUMAN RIGHTS LAW, GENEVA CALL, 74, 81 (2007).
A. *Ex Ante Recommendations*

1. Vetting

The state should vet any non-state actor with which it plans to work, along with its members. Depending on the context, this process may require national or international records from the host state, possibly including criminal records and civil complaints alleging human rights violations;\(^{177}\) psychological testing;\(^{178}\) mental health checks;\(^{179}\) and information collection on the ground, from social media, and from other public sources to the greatest extent practicable. If the non-state actor—or its members—has a history of violating international law, such that a violation in the future is reasonably foreseeable,\(^{180}\) the state should refrain from working with it.

---


178. DynCorp (a PMSC) and the French Foreign Legion engage in psychological testing as part of their vetting processes. *Id.* at 43.


180. For evidence of the “foreseeability of the event” standard used to determine state responsibility for failure to fulfill “to ensure respect” duties under the European Convention on
2. Training

Given that non-state actors often commit international law violations in part because they are unaware of them, a state should ensure that a non-state actor is aware of the applicable IHL. In some cases, this will require that the state assist in training the non-state actor. The Geneva Conventions require, moreover, that states disseminate the texts of the Conventions to relevant belligerents.

---


182. See Tonkin, supra note 145, at 796–98 (“The hiring state should also take steps to ensure that PMSC personnel are adequately trained and instructed in IHL. The obligation to ensure respect for IHL is commonly taken to include an obligation to ensure that national troops are trained and instructed in accordance with IHL standards. This would also require that a state ensure the training and instruction of any PMSCs it hires to perform military and security activities in armed conflict or occupation.”).

183. Geneva Convention I, supra note 10, art. 47; Geneva Convention II, supra note 10, art. 48; Geneva Convention III, supra note 10, art. 127; Geneva Convention IV, supra note 10, art. 144;
190 In implementing training programs, NGOs have emphasized the following best practices: (1) providing training that is not overly academic or theoretical, but rather, relevant to the given context;\textsuperscript{184} (2) focusing on particular norms rather than all norms generally (although there is disagreement among NGOs on this issue);\textsuperscript{185} (3) conducting training at the highest levels of command;\textsuperscript{186} (4) engaging former members of the non-state actor in developing the training;\textsuperscript{187} (5) engaging local populations in developing the training;\textsuperscript{188} and (6) emphasizing the legitimacy benefits of abiding by IHL.\textsuperscript{189}

\textit{see also} First Additional Protocol, supra note 10, art. 83 (affirming these provisions and obligations). These provisions should be interpreted to impose the requirement for states to disseminate the texts of the Geneva Conventions to non-state actors they are supporting. See Moyakine, supra note 78, at 314 (identifying and explaining dissemination provisions cited above); Tonkin, supra note 148, at 197–98 (explaining the function of dissemination provisions to inform non-state actors).

186. \textit{Id.} at 19; Bangerter, supra note 176, at 82.
187. ADH Report, supra note 181, at 35.
189. ADH Report, supra note 181, at 23 (noting that most non-state actors desire to be
3. Written Agreements

The state should have the non-state actor sign written agreements that the non-state actor will respect its international legal obligations. This recommendation addresses the fact that non-state actors often assert that they are not bound by IHL because they are not (and in most cases cannot be) parties to the relevant treaties.190 Having non-state actors sign written agreements provides another means to hold them accountable. It puts them on notice, moreover, that any support that is provided is contingent on continued compliance with IHL obligations.

NGOs have noted that these agreements can take different forms: (1) special agreements between parties to a conflict,191 (2) unilateral declarations that are made generally or to an NGO,192 and (3) codes of non-

---

190. ICRC REPORT, supra note 181, at 11; ADH Report, supra note 181, at 6–7, 7 n.13.


192. Bangerter, supra note 174, at 82–83; ICRC REPORT, supra note 179, at 19–21; ADH Report, supra note 179, at 34. As an example, Geneva Call has used this strategy, encouraging non-state actors to sign Deeds of Commitment renouncing the use of land mines and other tactics that violate IHL. GENEVA CALL REPORT, supra note 186, at 10.
state actor conduct that incorporate IHL. These agreements may also be analogized to contracts undertaken between states and PMSCs. When hiring PMSCs, scholars have suggested that exercising due diligence requires including contract provisions that stipulate PMSC personnel will follow IHL.

B. *Ex Post Recommendations*

1. Punishment Framework

The state should ensure that the non-state actor has an adequate punishment framework in place to deal with individuals who violate IHL. A similar concept is found in diplomatic protection law: The ILC has noted that, in that context, the due diligence obligation does not require successfully preventing a private actor from taking an action, but it does require taking "adequate protective measures" to prevent the action, and punishing the private actor if the action is taken.


194. See Tonkin, *supra* note 145, at 797 ("Another requirement of Common Article 1 is the inclusion of clear and appropriate rules of IHL in the contract of employment. Indeed, this represents the most direct way of imposing conditions on PMSC employees. Such contractual clauses should be accompanied by adequate procedures for supervising contractors in the field.").

195. See, e.g., MOYAKINE, *supra* note 78, at 360 (suggesting that countries employing PMSCs have a duty to create frameworks to address human rights violations arising out of their operations).

Many questions arise regarding what would constitute an "adequate" punishment framework. Although answering such questions in detail goes beyond the scope of this Article, the punishment framework should, at a minimum, include (1) oversight and monitoring;197 (2) investigation of alleged violations;198 (3) prosecution of alleged violators;199 and (4) punishment of convicted violators. This recommendation is a response to the concern that non-state actors often feel unconstrained by the law since they are already acting unlawfully by taking up arms against a state.

Implementing punitive frameworks with regard to non-state actors does, however, pose a number of challenges largely unaddressed in the literature. Presumably, punishment mechanisms must be compliant with IHL. There is

A/10010/Rev.1, at 71 (2012) (noting that although the acts of private actors are not directly attributable to the state, the state has a duty to reasonably protect against and deal with harm caused by its contractors); see also MOYAKINE, supra note 78, at 324 ("That the duty to punish might be understood as a broad international obligation to legislate, investigate, prosecute, punish, and provide redress appears to be quite clear.").

197. See MOYAKINE, supra note 78, at 324 (stating that the duty imposed upon states to take preventative measures to prevent abuses by non-state actors applies to PMSCs).

198. See id. (stating that the duty imposed upon states to investigate abuses by non-state actors applies to PMSCs).

199. In the context of Common Article 1 obligations for PMSCs, Tonkin suggests that this may also entail extradition. See Tonkin, supra note 145, at 798 ("[I]f the violation constitutes a criminal offence over which the hiring state has jurisdiction, the state should take steps to arrest and prosecute or extradite the perpetrator.").
little guidance or clarity to help determine whether non-Western forms of adjudication would be sufficient to meet the due process requirements under Common Article 3. Nevertheless, providing for some mechanism of accountability for non-state actor conduct may be essential for a state to exercise due diligence under Common Article 1.\textsuperscript{200}

2. Cessation of Support

The state should withdraw some or all of its support to the non-state actor if it is found to have breached a certain threshold of international law violations. A state is more likely to incur responsibility for breach of its Common Article 1 obligations for supporting a non-state actor that it knows is violating IHL.

A single violation would not necessarily require a cessation of support. If the primary obligations owed by the state are due diligence obligations, Article 14(3) of the Draft Articles arguably comes into play. Article 14(3) provides: "The breach of an international obligation requiring a State to prevent a given event occurs when the event occurs and extends over the entire period during which the event continues and remains not in conformity with that obligation."\textsuperscript{201} The state might decide that it is appropriate to give

\begin{flushleft}
\textsuperscript{200} The ICJ considered punishment a requirement of international obligations in \textit{Bosnian Genocide}. \textit{Bosnian Genocide}, 2007 I.C.J., ¶ 439.
\end{flushleft}

\begin{flushleft}
\textsuperscript{201} \textsc{Moyakine}, \textit{supra} note 79, 325–26 ("The positive measures to be taken by States may
\end{flushleft}
the non-state actor an opportunity to respond to the violation to prevent it from recurring.

Conclusion

Today, states are increasingly working with and through non-state actors in a range of contexts. As a result, there is a real and growing danger that states will use non-state actors to avoid their international legal obligations. The leading legal framework for addressing this danger—modern attribution doctrine—adopts a bright line rule: a state is responsible, or it is not. This, in turn, has generated a set of perverse incentives for states that collaborate with non-state actors in armed conflict situations, granting them virtually free reign below the attribution threshold while discouraging them from exercising responsible control that might push them over the threshold. If the purpose of state responsibility doctrine is to encourage states to engage responsibly with non-state partners and hold states accountable by punishing bad actors, the existing framework falls dangerously short.

The more robust interpretation of Common Article I of the Geneva Conventions recently endorsed by the ICRC in its landmark new Commentaries could help address this shortcoming, closing much of the

include the duty to intervene when a violation of international law is likely to occur and to regulate the activities of private actors in order to prevent breaches of international humanitarian law and human rights law.”).
accountability gap left by modern attribution doctrine in armed conflict situations. Rightly understood, Common Article 1’s “to ensure respect” provision requires states to take steps to prevent non-state actors from violating IHL, even when they do not exercise effective or overall control over them. Failure to exercise due diligence to prevent non-state partners’ IHL violations constitutes an independent source of state responsibility.

Although Common Article 1 goes a long way toward closing the accountability gap, it does not fully resolve the incentives problem. States that instruct, train, and equip their non-state partners in an effort to fulfill their Common Article 1 duties are more likely to cross the threshold for attribution liability than states that eschew such prophylactic measures.202 In part as a result, states have already expressed reluctance to accept the positive obligations entailed in the new Commentaries.203 To address this concern, states that take actions to meet their due diligence obligations under Common Article 1 should be permitted to plead an affirmative defense: If a state has exercised due diligence to ensure non-state actors abide by the Geneva

202. See supra Part IV.

203. For a discussion of U.S. State Department Legal Advisor Brian Egan’s early reaction to the publication of the new Commentaries, see Oona Hathaway & Zachary Manfredi, The State Department Adviser Signals a Middle Road on Common Article 1, JUST SECURITY (Apr. 12, 2016) https://www.justsecurity.org/30560/state-department-adviser-signals-middle-road-common-article-1/ [https://perma.cc/RVT5-LLXC].
Conventions, and those actors nevertheless do commit *ultra vires* violations, the state should not be held responsible. This innovation would not only comport with common sense, but it would encourage states to embrace the ICRC’s more robust reading of Common Article 1 and take reasonable measures to ensure that their partner non-state actors comply with international law.
PANEL II:

THE NATIONAL SECURITY PROCESS AND STRUCTURE

MODERATOR:

JOHN NORTON MOORE
POLICY ADDRESS: “LEGAL FRAMEWORK FOR THE
U.S. USE OF MILITARY FORCE SINCE 9/11”

This policy address was given at 5:00 p.m., Friday, April 10. The speaker was Stephen
Preston of the U.S. Department of Defense.

REMARKS BY STEPHEN PRESTON*

Thank you, Professor Damrosch, for that kind introduction and for the invitation to be
here this afternoon. As a leader in ASIL, a professor of international law, and for many
years editor of the American Journal of International Law, you have played a central role
in shaping our understanding of international law. And you have done so with an eye to the
practical realities faced by the government lawyer, which has made your contributions all
the more meaningful. I also want to thank Mark Agrast and Wes Rist, who have done so
much to make this event, and my participation in it, possible.

I am grateful, as well, to my colleagues in government, who have contributed to my
remarks today in many ways—not least through the wisdom, learning, and hard work they
have brought to bear in answering the difficult questions we regularly face together. Finally,
I want to thank all of you—the members of the American Society of International Law
assembled here this afternoon—for the warm reception I have received and, more important,
for your keen interest in the legal issues affecting the national security of our country. I am
very pleased to have the opportunity to speak with you today. Indeed, I am greatly honored.

The Department of Defense has a long history of engagement with the American Society
of International Law. The first and longest-serving president of the Society, Elihu Root,
served as Secretary of War under two presidents before founding the Society in 1906. He
saw this organization as a place where the hard issues of the day could be discussed and
debated. And he believed that by educating the American public about international law,
the rush to war could be slowed. As he once put it, “[i]n the great business of settling international
controversies without war . . . essential conditions are reasonableness and good temper, a
willingness to recognize facts and to weigh arguments which make against one’s own country
as well as those which make for one’s own country.” I could not agree more.

The theme of this year’s annual meeting, “Adapting to a Rapidly Changing World,” is
a pretty good description of our day-to-day job at the Defense Department. The conflicts
and threats we face are constantly shifting and evolving. Today, I will discuss how the U.S.
government has responded to this rapidly changing world and, specifically, how the legal
framework for our military operations has developed since the attacks of 9/11.

INTRODUCTION

President Obama has made clear from the beginning of his presidency that he is deeply
committed to transparency in government because it strengthens our democracy and promotes
accountability. Although a certain degree of secrecy is of course required to protect our

* Formerly General Counsel of the Department of Defense and is currently a partner in the law firm of Wilmer
Cutler Pickering Hale and Dorr LLP. He wishes to acknowledge the assistance of Professor Oona Hathaway of
Yale Law School in the preparation of these remarks while she was serving as Special Counsel to the General
Counsel for National Security Law. No copyright is claimed in the content of these remarks, which were delivered
by a federal official in his official capacity.

1 Elihu Root, The Need of Popular Understanding of International Law, 1 AJIL 1, 2 (1907).
country, the administration has demonstrated its commitment to greater transparency in matters of national security and, specifically, in explaining the bases, under domestic and international law, for the United States’ use of military force abroad. We have seen this in the president’s own speeches, for example, at the National Archives in May 2009, at National Defense University (NDU) in May 2013, and at West Point in May 2014.

Among senior administration lawyers, we saw this early on, in a speech by the State Department’s Legal Adviser at ASIL in March 2010—this same meeting, five years ago—and in later speeches by the Attorney General at Northwestern in March 2012, and by my predecessor as Department of Defense General Counsel at Yale and at Oxford, both in 2012. There was even a very modest contribution by the CIA General Counsel in remarks at Harvard Law School in April 2012. My remarks here today are the latest in the series—an update of sorts—addressing the legal authority for U.S. military operations as the mission has evolved over the past year or so.

This talk will proceed in four parts. First, I want to review the legal framework for the use of military force developed in the aftermath of the 9/11 attacks. Second, I will explain the legal basis for current military operations against the so-called Islamic State of Iraq and the Levant, or ISIL. Third, I will discuss the end of the U.S. combat mission in Afghanistan and its impact on the legal basis for the continuing use of military force under the 2001 AUMF. Fourth, and finally, I will look ahead to the legal framework for counterterrorism operations in the future.

LEGAL FRAMEWORK DEVELOPED IN THE AFTERMATH OF THE ATTACKS

Let us begin with a bit of history. It is only by seeing where we have been over the past decade and a half that we can understand where we are today.

Return to the first days after the attacks on September 11, 2001, for it is in that time that our government began to articulate the legal framework that we still rely on today. As many of you know, it was only days after the 9/11 attacks that Congress passed, and the president signed, an authorization for the use of military force, or AUMF, authorizing the president to take action to protect the United States against those who had attacked us. Even though it was only days later, we already knew that the attacks were the work of Al Qaeda, a terrorist organization operating out of Afghanistan, led by a man named Usama bin Laden. The authorization that was enacted into law—which came to be known as the 2001 AUMF—was not a traditional declaration of war against a state. We had been attacked, instead, by a terrorist organization. Yes, the Taliban had allowed bin Laden and his organization to operate with impunity within Afghanistan. But it was not Afghanistan that had launched the attack. It was bin Laden and his terrorist organization.

The authorization for the use of military force that Congress passed aimed to give the president all the statutory authority he needed to fight back against bin Laden, his organization, and those who supported him, including the Taliban. At the same time, the 2001 AUMF was not without limits. It authorized the president to “use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.”2

Policy Address: "Legal Framework for the U.S. Use of Military Force Since 9/11"

With this statutory authorization, the United States commenced military operations against Al Qaeda and the Taliban in Afghanistan on October 7, 2001, notifying the UN Security Council consistent with Article 51 of the UN Charter that the United States was taking action in the exercise of its right of self-defense in response to the 9/11 attacks.

Although the 2001 AUMF was not unlimited, enacted as it was just a short time after the attacks, it was necessarily drafted in broad terms. Shortly after President Obama came into office, his administration filed a memorandum in Guantánamo habeas corpus litigation offering the new president's interpretation of his statutory authority to detain enemy forces as an aspect of his authority to use force under the 2001 AUMF. That memorandum explained that the statute authorized the detention of "persons who were part of, or substantially supported, Taliban or Al Qaeda forces or associated forces that are engaged in hostilities against the United States or its coalition partners, including any person who has committed a belligerent act, or has directly supported hostilities, in aid of such enemy armed forces."3 Moreover, it stated that "[p]rinciples derived from law-of-war rules governing international armed conflicts . . . must inform the interpretation of the detention authority Congress has authorized" under the AUMF.4

This interpretation of the 2001 AUMF was adopted by the D.C. Circuit and, in 2011, it was expressly endorsed by Congress in the context of detention. The National Defense Authorization Act for Fiscal Year 2012 reaffirmed the authority to detain "[a] person who was a part of or substantially supported al-Qaeda, the Taliban, or associated forces that are engaged in hostilities against the United States or its coalition partners, including any person who has committed a belligerent act or has directly supported such hostilities in aid of such enemy forces."5 It also reaffirmed that dispositions of such individuals are made "under the law of war." Thus, a decade after the conflict began, all three branches of the government weighed in to affirm the ongoing relevance of the 2001 AUMF and its application not only to those groups that perpetrated the 9/11 attacks or provided them safe haven, but also to certain others who were associated with them.

My predecessor, Jeh Johnson, later elaborated on the concept of associated forces. In a speech at Yale Law School in February 2012, he explained that the concept of associated forces is not open-ended. He pointed out that, consistent with international law principles, an associated force must be both (1) an organized, armed group that has entered the fight alongside Al Qaeda, and (2) a co-belligerent with Al Qaeda in hostilities against the United States or its coalition partners. This means that not every group that commits terrorist acts is an associated force. Nor is a group an associated force simply because it aligns with Al Qaeda. Rather, a group must have also entered Al Qaeda’s fight against the United States or its coalition partners.

More recently, during a public hearing before the Senate Foreign Relations Committee in May 2014, I discussed at some length the executive branch’s interpretation of the 2001 AUMF and its application by the Department of Defense in armed conflict. In my testimony, I described in detail the groups and individuals against which the U.S. military was taking direct action (that is, capture or lethal operations) under the authority of the 2001 AUMF, including associated forces. Those groups and individuals are: Al Qaeda, the Taliban, and

3 In re Guantánamo Bay Detainee Litigation, Misc. No. 08-0442, Respondents' Memorandum Regarding the Government’s Detention Authority Relative to Detainees Held at Guantánamo Bay, 2 (D.D.C. Mar. 13, 2009).
4 Id. at 1.
certain other terrorist or insurgent groups in Afghanistan; Al Qaeda in the Arabian Peninsula (AQAP) in Yemen; and individuals who are part of Al Qaeda in Somalia and Libya. In addition, over the past year, we have conducted military operations under the 2001 AUMF against the Nusrah Front and, specifically, those members of Al Qaeda referred to as the Khorasan Group in Syria. We have also resumed such operations against the group we fought in Iraq when it was known as Al Qaeda in Iraq, which is now known as ISIL.

The concept of associated forces under the 2001 AUMF does not provide the president with unlimited flexibility to define the scope of his statutory authority. Our government monitors the threats posed to the United States and maintains the capacity to target (or stop targeting) groups covered by the statute as necessary and appropriate. But identifying a new group as an associated force is not done lightly. The determination that a particular group is an associated force is made at the most senior levels of the U.S. Government, following reviews by senior government lawyers and informed by departments and agencies with relevant expertise and institutional roles, including all-source intelligence from the U.S. intelligence community. In addition, military operations against these groups are regularly briefed to Congress. There are no other groups—other than those publicly identified, as I have just described—against which the U.S. military is currently taking direct action under the authority of the 2001 AUMF.

LEGAL BASIS FOR CURRENT MILITARY OPERATIONS AGAINST ISIL

That brings me to my second topic: the legal authority applicable to today’s fight against ISIL. The military operations conducted by the United States against ISIL in Iraq and Syria are consistent with both domestic and international law.

First, a word about this group we call ISIL, referred to variously as ISIS, the Islamic State or Daesh (its acronym in Arabic). In 2003, a terrorist group founded by Abu Mu'sab al-Zarqawi—whose ties to bin Laden dated from al-Zarqawi’s time in Afghanistan and Pakistan before 9/11—conducted a series of sensational terrorist attacks in Iraq. These attacks prompted bin Laden to ask al-Zarqawi to merge his group with Al Qaeda. In 2004, al-Zarqawi publicly pledged his group’s allegiance to bin Laden, and bin Laden publicly endorsed al-Zarqawi as Al Qaeda’s leader in Iraq. For years afterwards, al-Zarqawi’s group, often referred to as Al Qaeda in Iraq, or AQI for short, conducted numerous deadly terrorist attacks against U.S. and coalition forces, as well as Iraqi civilians, using suicide bombers, car bombs, and executions. In response to these attacks, U.S. forces engaged in combat—at times, near daily combat—with the group from 2004 until U.S. and coalition forces left Iraq in 2011. Even since the departure of U.S. forces from Iraq, the group has continued to plot attacks against U.S. persons and interests in Iraq and the region—including the brutal murder of kidnapped American citizens in Syria and threats to U.S. military personnel in Iraq.

The 2001 AUMF has authorized the use of force against the group now called ISIL since at least 2004, when bin Laden and al-Zarqawi brought their groups together. The recent split between ISIL and current Al Qaeda leadership does not remove ISIL from coverage under the 2001 AUMF, because ISIL continues to wage the conflict against the United States that it entered into when, in 2004, it joined bin Laden’s Al Qaeda organization in its conflict against the United States. As AQI, ISIL had a direct relationship with bin Laden himself and waged that conflict in allegiance to him while he was alive. ISIL now claims that it, not Al Qaeda’s current leadership, is the true executor of bin Laden’s legacy. There are rifts between ISIL and parts of the network bin Laden assembled, but some members and factions of Al Qaeda-aligned groups have publicly declared allegiance to ISIL. At the same time,
ISIL continues to denounce the United States as its enemy and to target U.S. citizens and interests.

In these circumstances, the president is not divested of the previously available authority under the 2001 AUMF to continue protecting the country from ISIL—a group that has been subject to that statute for close to a decade—simply because of disagreements between the group and Al Qaeda’s current leadership. A contrary interpretation of the statute would allow the enemy—rather than the president and Congress—to control the scope of the AUMF by splintering into rival factions while continuing to prosecute the same conflict against the United States.

Some initially greeted with skepticism the president’s reliance on the 2001 AUMF for authority to renew military operations against ISIL last year. To be sure, we would be having a different conversation if ISIL had emerged out of nowhere a year ago, having no history with bin Laden and no more connection to current Al Qaeda leadership than it has today, or if the group once known as AQI had, for example, renounced terrorist violence against the United States at some point along the way. But ISIL did not spring fully formed from the head of Zeus a year ago, and the group certainly has never laid down its arms in its conflict against the United States.

The name may have changed, but the group we call ISIL today has been an enemy of the United States within the scope of the 2001 AUMF continuously since at least 2004. A power struggle may have broken out within bin Laden’s jihadist movement, but this same enemy of the United States continues to plot and carry out violent attacks against us to this day. Viewed in this light, reliance on the AUMF for counter-ISIL operations is hardly an expansion of authority. After all, how many new terrorist groups have, by virtue of this reading of the statute, been determined to be among the groups against which military force may be used? The answer is zero.

The president’s authority to fight ISIL is further reinforced by the 2002 authorization for the use of military force against Iraq (referred to as the 2002 AUMF). That AUMF authorized the use of force to, among other things, “defend the national security of the United States against the continuing threat posed by Iraq.” Although the threat posed by Saddam Hussein’s regime in Iraq was the primary focus of the 2002 AUMF, the statute, in accordance with its express goals, has long been understood to authorize the use of force for the related purposes of helping to establish a stable, democratic Iraq and addressing terrorist threats emanating from Iraq. After Saddam Hussein’s regime fell in 2003, the United States, with its coalition partners, continued to take military action in Iraq under the 2002 AUMF to further these purposes, including action against AQI, which then, as now, posed a terrorist threat to the United States and its partners and undermined stability and democracy in Iraq. Accordingly, the 2002 AUMF authorizes military operations against ISIL in Iraq and, to the extent necessary to achieve these purposes, in Syria.

Beyond the domestic legal authorities, our military operations against ISIL have a firm foundation in international law, as well. The U.S. government remains deeply committed to abiding by our obligations under the applicable international law governing the resort to force and the conduct of hostilities. In Iraq, of course, the United States is operating against ISIL at the request and with the consent of the government of Iraq, which has sought U.S. and coalition support in its defense of the country against ISIL. In Syria, the United States

---

is using force against ISIL in the collective self-defense of Iraq and U.S. national self-defense, and it has notified the UN Security Council that it is taking these actions in Syria consistent with Article 51 of the UN Charter. Under international law, states may defend themselves, in accordance with the inherent right of individual and collective self-defense, when they face armed attacks or the imminent threat of armed attacks and the use of force is necessary because the government of the state where the threat is located is unwilling or unable to prevent the use of its territory for such attacks.

The inherent right of self-defense is not restricted to threats posed by states, and over the past two centuries states have repeatedly invoked the right of self-defense in response to attacks by non-state actors. Iraq has been clear, including in letters it has submitted to the UN Security Council, that it is facing a serious threat of continuing armed attacks from ISIL coming out of safe havens in Syria, and it has asked the United States to lead international efforts to strike ISIL sites and strongholds in Syria in order to end the continuing armed attacks on Iraq, to protect Iraqi citizens and ultimately enable Iraqi forces to regain control of Iraqi borders. ISIL is a threat not only to Iraq and our partners in the region, but also to the United States. Finally, the Syrian government has shown that it cannot and will not confront these terrorist groups effectively itself.

The End of the U.S. Combat Mission in Afghanistan

Let us turn now to my third topic: the end of the U.S. combat mission in Afghanistan and its impact on the legal basis for the continuing use of military force under the 2001 AUMF.

At the outset, I pause to observe, as Clemenceau put it, “It is far easier to make war than to make peace.” That remains as true today as it was a hundred years ago. Indeed, in an armed conflict between a state and a terrorist organization like Al Qaeda or ISIL, it is highly unlikely that there will ever be an agreement to end the conflict. Unlike at the close of the World Wars, there will not be any instruments of surrender or peace treaties.

The situation is further complicated by the fact that the U.S. Constitution says nothing directly about how wars are to be ended. The closest it comes is the Treaty Clause, which gives the president and the Senate the power, together, to join treaties—which were, at the time the Constitution was written, the main way that wars were brought to an end. But, again, for a variety of reasons, the current conflict is unlikely to end in that way.

How, then, are we to know when the armed conflict has come to an end? The Supreme Court has not directly addressed this question, but it has offered important guidance. In Hamdi v. Rumsfeld, the plurality interpreted the 2001 AUMF as informed by the international law of war. Citing Article 118 of the Third Geneva Convention, it explained, “[i]t is a clearly established principle of the law of war that detention may last no longer than active hostilities.” It concluded, “[t]he United States may detain, for the duration of these hostilities, individuals legitimately determined to be Taliban combatants who engaged in an armed conflict against the United States.” Consistent with the Court’s approach, the Obama administration has interpreted the AUMF as informed by these international law principles, and this interpretation has been embraced by the federal courts. Hence, where the armed conflict remains ongoing and active hostilities have not ceased, it is clear that congressional authorization to detain and use military force under the 2001 AUMF continues.

8 Id.
Now what does this mean for U.S. military operations in Afghanistan after 2014? Although our presence in that country has been reduced and our mission there is more limited, the fact is that active hostilities continue. As a matter of international law, the United States remains in a state of armed conflict against the Taliban, Al Qaeda, and associated forces, and the 2001 AUMF continues to stand as statutory authority to use military force.

At the end of last year, the president made clear that “our combat mission in Afghanistan is ending, and the longest war in American history is coming to a responsible conclusion.” As a part of this transition, we have drawn down our forces to roughly 10,000—the fewest U.S. forces in Afghanistan in more than a decade. The U.S. military now has two missions in Afghanistan. First, the United States is participating in the NATO non-combat mission of training, advising, and assisting the Afghan National Security Forces. Second, the United States continues to engage in counterterrorism activity in Afghanistan to target the remnants of Al Qaeda and prevent an Al Qaeda resurgence or external plotting against the homeland or U.S. targets abroad. With respect to the Taliban, U.S. forces will take appropriate measures against Taliban members who directly threaten U.S. and coalition forces in Afghanistan, or provide direct support to Al Qaeda. The use of force by the U.S. military in Afghanistan is now limited to circumstances in which using force is necessary to execute those two missions or to protect our personnel.

At the same time, our military operations in Afghanistan remain substantial. Indeed, the president recently announced that U.S. force levels in Afghanistan will draw down more slowly than originally planned because Afghanistan remains a dangerous place. It is sometimes said that the enemy gets a vote. Taliban members continue to actively and directly threaten U.S. and coalition forces in Afghanistan, provide direct support to Al Qaeda, and pose a strategic threat to the Afghan National Security Forces. In response to these threats, U.S. forces are taking necessary and appropriate measures to keep the United States and U.S. forces safe and assist the Afghans. In short, the enemy has not relented, and significant armed violence continues.

The United States’ armed conflict against Al Qaeda and associated forces in Afghanistan and elsewhere also continues. As my predecessor explained at the Oxford Union in 2012, there will come a time when so many of the leaders and operatives of Al Qaeda and its affiliates have been killed or captured, and the group is no longer able to attempt or launch a strategic attack against the United States, such that Al Qaeda as we know it has been effectively destroyed. Unfortunately, that day has not yet come. To be sure, progress has been made in disrupting and degrading Al Qaeda, particularly its core, senior leadership in the tribal areas along the Afghanistan-Pakistan border. But Al Qaeda and its militant adherents—including AQAP, that most virulent strain of Al Qaeda in Yemen—still pose a real and profound threat to U.S. national security—one that we cannot and will not ignore.

Because the Taliban continues to threaten U.S. and coalition forces in Afghanistan, and because Al Qaeda and associated forces continue to target U.S. persons and interests actively, the United States will use military force against them as necessary. Active hostilities will continue in Afghanistan (and elsewhere) at least through 2015 and perhaps beyond. There is no doubt that we remain in a state of armed conflict against the Taliban, Al Qaeda, and associated forces as a matter of international law. And the 2001 AUMF continues to provide the president with domestic legal authority to defend against these ongoing threats.

Finally, we have come to my fourth topic: the future of the legal framework governing the United States' use of military force. I have described for you how we arrived where we are over the course of nearly fourteen years. The 2001 AUMF continues to provide authority for our ongoing military operations against Al Qaeda, ISIL, and others, even though the conditions of the fight have changed since that authorization was first enacted.

In his 2013 NDU speech, the president anticipated “engaging Congress and the American people in efforts to refine, and ultimately repeal, the AUMF’s mandate.” While, today, the administration’s immediate focus is to work with Congress on a bipartisan, ISIL-specific AUMF, the president’s position on the 2001 statute has not changed. When transmitting to Congress his draft AUMF against ISIL, he stated, “Although my proposed AUMF does not address the 2001 AUMF, I remain committed to working with Congress and the American people to refine, and ultimately repeal, the 2001 AUMF,” that is, to tailor the authorities granted by the AUMF to better fit the current fight and the strategy going forward. Our democracy is at its best when we openly debate matters of national security, and our nation is strongest when the president and Congress are in agreement on the employment of military force in its defense. The president has made clear that he stands ready to work with Congress to refine the 2001 AUMF after enactment of an ISIL-specific AUMF.

In February of this year, President Obama submitted to Congress draft legislation authorizing use of “the Armed Forces of the United States as the president determines to be necessary and appropriate against ISIL or associated persons or forces.” This raises the question: if the president already has the authority needed to take action against ISIL, why is he seeking a new authorization?

Most obviously and importantly, as the president has said, the world needs to know we are united behind the effort against ISIL, and the men and women of our military deserve our clear and unified support. Enacting the president’s proposed AUMF will show our fighting forces, the American people, our foreign partners, and the enemy that the president and Congress are united in their resolve to degrade and defeat ISIL.

But the value of having a new authorization expressly directed against ISIL and associated forces of ISIL extends beyond its expression of the political branches’ unified support for our counter-ISIL efforts. The 2001 and 2002 AUMFs authorize the current military operations against ISIL, but they were enacted more than a decade ago. The last fourteen years have taught us that the threats we face tomorrow will not be the same as the threats we faced yesterday or face today. This confrontation with ISIL will not be over quickly, and now is an appropriate time for the president, Congress, and the American people to define the scope of the conflict and make sure we have the appropriate authorities in place for the counter-ISIL fight.

To that end, the president has made clear that as part of the counter-ISIL mission he will not deploy U.S. forces to engage in long-term, large-scale ground combat operations like those our nation conducted in Iraq and Afghanistan. With its proposed AUMF, the administration has

---


sought to strike a balance, putting in place reasonable limitations that would, as the president said at NDU, "discipline our thinking, our definition, [and] our actions," while continuing to provide the authority and flexibility needed to accomplish the mission and preserve the Commander in Chief's authority to respond to unforeseen circumstances. And by working with Congress and the American people to come up with appropriate authorizing legislation for the fight against ISIL, we might also create a model to guide future efforts to refine the 2001 AUMF or otherwise authorize the use of force against some new threat we may not yet foresee.

A central question as we look ahead is what follow-on legal framework will provide the authorities necessary in order for our government to meet the terrorist threat to our country, but will not greatly exceed what is needed to meet that threat. Drawing again from the president's NDU speech, the answer is not legislation granting the Executive "unbound powers more suited for traditional armed conflicts between nations." Rather, the objective is a framework that will support "a series of persistent, targeted efforts to dismantle specific networks of violent extremists that threaten America." The challenge is to ensure that the authorities for U.S. counterterrorism operations are both adequate and appropriately tailored to the present and foreseeable threat.

Of course, in conducting military operations under the authority of existing AUMFs, a new, ISIL-specific AUMF, or a follow-on framework designed to replace the 2001 AUMF, we will remain committed to acting in accordance with our international obligations. As I have already described, our actions against ISIL in Iraq and Syria are justified as a matter of international law, and our military operations are being carried out in accordance with the law of armed conflict. This will continue to be the case under any new domestic authorizations.

CONCLUSION

As a law partner of mine used to say, I go out the door I came in: I would like to close with a few words about transparency in matters of law and national security.

At the time I returned to government, in 2009, I could not pick up a newspaper or turn on a news broadcast without seeing erroneous references to "illegal" U.S. government counterterrorism operations overseas. Not fringe media, but mainstream press. Not isolated or occasional instances, but quite routine—as if it were conventional wisdom that the United States' use of lethal force in the armed conflict against Al Qaeda was "unlawful." For me, and others in the administration, this was deeply disturbing, and something had to be done about it. The something that was done about it was the series of speeches that I mentioned at the outset of my remarks. It all began at this very meeting in 2010, with Harold Koh's defense of U.S. counterterrorism operations in which he identified the international and domestic legal bases for lethal operations, including the use of remotely piloted aircraft. And it continued with the speeches that followed, including Eric Holder's 2012 Northwestern speech, again noting the domestic and international legal authorities for U.S. counterterrorism operations and carefully explaining how citizenship does not confer immunity on one who takes up arms against our country. Repeatedly, in court filings as well as these speeches, the administration has sought to explain the legal rationale for the actions it has taken.

13 Presidential Remarks at NDU, supra note 10.
15 Id.
One result: You no longer find, in the popular press or in professional discourse, the same routine references to the U.S. government's counterterrorism operations as being "illegal." Not that the administration has persuaded everyone or will ever satisfy all of its critics. But the lawfulness of our government's efforts to counter foreign terrorist threats is now better understood, and more widely accepted, at home and abroad.

Transparency to the extent possible in matters of law and national security is sound policy and just plain good government. As noted earlier, it strengthens our democracy and promotes accountability. Moreover, from the perspective of a government lawyer, transparency, including clarity in articulating the legal bases for U.S. military operations, is essential to ensure the lawfulness of our government's actions and to explain the legal framework on which we rely to the American public and our partners abroad. Finally, I firmly believe transparency is important to help inoculate, against legal exposure or misguided recriminations, the fine men and women the government puts at risk in order to defend our country. We agency counsel all serve the same client, the United States of America, and each of us answers to the head of our respective agencies. But our highest calling, in my personal view, is to serve those who serve us.

Ladies and gentlemen: If my remarks this afternoon, like the speeches in past years, go any distance towards furthering public understanding and protecting those in uniform who are protecting us, I will have done what I set out to do. I thank you for listening. And I want to thank for your continued support of the men and women serving us in the United States Armed Forces.
The National Security Policy Process:
The National Security Council and Interagency System

By
Alan G. Whittaker, Ph.D
Shannon A. Brown, Ph.D
Frederick C. Smith,
and Ambassador Elizabeth McKune

Annual Update: August 15, 2011
Table of Contents

EVOLUTION OF THE NATIONAL SECURITY SYSTEM ......................................................................................................................... 6
NSC ORGANIZATION .............................................................................................................................................................................. 12
National Security Staff ............................................................................................................................................................................. 19
Homeland Security Council ....................................................................................................................................................................... 20
National Economic Council ....................................................................................................................................................................... 23
NSC POLICY PROCESS ........................................................................................................................................................................... 24
The National Security Advisor and the Policy Process .................................................................................................................. 25
The National Security Staff and the Policy Process ......................................................................................................................... 29
Principals and Deputies Committees and the Policy Process ........................................................................................................ 31
Interagency Policy Committees and the Policy Process .................................................................................................................. 34
The HSC and the Policy Process ........................................................................................................................................................... 42
KEY DEPARTMENTS AND AGENCIES IN THE NATIONAL SECURITY POLICY PROCESS .................................................................................. 44
Department of State ................................................................................................................................................................................ 44
Department of Defense ............................................................................................................................................................................. 48
The Intelligence Community .................................................................................................................................................................... 58
Homeland Security .................................................................................................................................................................................. 60
Department of Homeland Security ....................................................................................................................................................... 61
APPENDIX A. Presidential National Security Policy Decision Documents ............................................................................................... 66
APPENDIX B. Assistants to the President for National Security Affairs ............................................................................................................ 67
APPENDIX C: Obama Administration PPDs and PSDs .......................................................................................................................... 68
APPENDIX D: National Security Staff organizational chart ............................................................................................................... 69
APPENDIX E: Department of State organizational chart .......................................................................................................................... 70
APPENDIX F: Department of Defense organizational chart .................................................................................................................... 71
APPENDIX G: NORTHCOM organizational chart ........................................................................................................................................ 72
APPENDIX H: Intelligence Community organizational chart .................................................................................................................. 73
APPENDIX I: Department of Homeland Security organizational chart .................................................................................................. 74
ENDNOTES ...................................................................................................................................................................................................... 75

Feedback or corrections should be sent to: browns@ndu.edu

On-line location for this report: http://www.ndu.edu/icaf/ under “Reports and Publications.”

Citation format for this report:
The National Security Policy Process: 
The National Security Council and Interagency System

By
Alan G. Whittaker, Shannon A. Brown, Frederick C. Smith, and Elizabeth McKune

How United States' foreign, defense, and other national security policies are developed, coordinated, articulated, and implemented is critically important to this nation's well being. This process begins internally with the federal agencies responsible for our national security and culminates with the President ultimately making the decisions. To do this, the President needs a defined and smoothly functioning policy development and decision-making process. Other than an extremely broad outline of who should participate in the process, there are no laws or regulations directing how policy decisions should be made. Much depends upon personalities and the strengths and weaknesses of the people who work for the President, as well as the personality and management style of the President himself.

Central to the policy development and decision-making process is the National Security Council (NSC) which serves as the President's principal forum for considering national security and foreign policy matters with his senior national security advisors and cabinet officials. The NSC advises and assists the President on national security and foreign policies and serves as the President's principal arm for coordinating these policies among various government agencies.1 The Homeland Security Council (HSC) is a complementary body of

---

1 Dr. Alan G. Whittaker is the former Dean of Faculty and Academic Programs at the Industrial College of the Armed Forces, National Defense University and previously served as a Political Psychologist for the CIA.
Dr. Shannon A. Brown is a Professor of National Security Studies at the Industrial College of the Armed Forces, National Defense University.
Frederick C. Smith is a former Deputy Assistant Secretary of Defense, served over 30 years in the Department of Defense, and is a veteran of numerous interagency deliberations.
Ambassador Elizabeth McKune is a retired career Foreign Service Officer who has served as the State Department's Deputy Executive Secretary, and also was U.S. Ambassador to the State of Qatar from 1998-2001.

The authors are indebted to Leonard H. Hawley, whose experiences as a Deputy Assistant Secretary at both DOD and the State Department, and as an NSC Director provided numerous insights into interagency dynamics, objectives, and lessons; to Nate Tibbits, Executive Secretary, National Security Council, and Douglas A. Koneff and Valerie Smith Boyd, Deputy Exec Secretaries, NSS; Phil McNamara, Department of Homeland Security Executive Secretary; Don Swain, DHS Deputy Exec Sec, Juliana Talaro, DHS Exec Sec Director of White House Actions and Mark Dolan, Plans Director, DHS OPS; The Office of the Director of National Intelligence; Saadia Sarkis, Interagency Coordinator, State Department Secretariat; Barry Cardwell, NORAD-USNORTHCOM, and Jan P. Ithier, Deputy Director, NORAD-USNORTHCOM Washington Office for their collaboration, review, and coordination of the 2011 report.
cabinet officials established to advise the President on preparedness and response to potential threats against the homeland. Together, the personnel supporting the NSC and the HSC are referred to as the National Security Staff.

This report provides an annually updated description of the national security decision-making process of the U.S. government. Although decisions affecting our security have been made since the nation's birth, the foundations of the current system were laid following World War II with the National Security Act of 1947. This report briefly summarizes how the process has evolved since its creation under President Truman. It describes the current NSS organizational structure and processes, and defines the roles of the key departments and agencies, including that of the National Security Staff. Readers should keep in mind that the processes described in this report reflect, in general, the operation of the national security interagency system. However, at times, individuals and circumstances have produced idiosyncratic ways of doing business. Finally, the report discusses how the interagency process is incorporating the relatively new organizational structures associated with homeland defense and homeland security.

EVOLUTION OF THE NATIONAL SECURITY SYSTEM

The national security decision-making process is critical to the management of the national security interests of the United States. When the President makes foreign policy statements, meets with visiting heads of state, travels abroad, or holds press conferences dealing with national security his words usually have been carefully crafted and are the result of lengthy and detailed deliberations within the administration. U.S. presidents have been supported by some kind of interagency policymaking process in the United States government since World War I. The current interagency system involving the routine consultations of senior department and agency officials, however, was not the creation of the President or the Executive Branch. Initially, in 1947, the National Security Council was an unwanted bureaucracy imposed upon the President by Congress, and was both little used and viewed with suspicion by the chief executive.

At the end of World War II, Congress sought to pass legislation that would, in part, reorganize the conduct of national security affairs for the U.S. government to ensure that a surprise attack upon the United States, such as that inflicted at Pearl Harbor, would never again occur. President Harry S Truman supported some kind of reorganization. When looking at the disparate pieces of information available to different elements of the United States government prior to December 7, 1941, President Truman was reported to have concluded, “If we'd all had that information in one agency, by God, I believe we could have foreseen what was going to happen in Pearl Harbor.” To put this in a current context, Truman's reaction and goals were not unlike those raised by The National Commission on Terrorist Attacks Upon the United States (also known as
the 9-11 Commission\textsuperscript{5} in evaluating the deficiencies in interagency collaboration and coordination which preceded the terrorist attacks of September 11\textsuperscript{th}. Moreover, the attacks of 2001 reflect the new post-Cold War challenges for the various components of the U.S. national security community in monitoring dispersed, non-state actors using asymmetric tactics.

Truman supported Congress's desire to establish a permanent, centrally managed intelligence community and a unified Department of Defense. But Congress also wanted an apparatus in the Executive Branch to ensure integration and coordination of policies across departments and agencies, and to advise the president on national security interests. As a result of Pearl Harbor, but also in reaction to President Roosevelt's highly personalized management of policy during World War II, Congress established a formal national security structure that was codified in the National Security Act of 1947.\textsuperscript{6} Congress believed that if formal interagency consultative structures were established, intelligence and policy would be better coordinated, and experienced voices would be present to advise the President on important decisions.

President Truman agreed with the intelligence and defense aspects of the legislation, and agreed to the need for an established advisory group, but was resistant to the idea of creating any other organization with decision-making authority or operational responsibilities within the Executive Branch.\textsuperscript{7} Truman fully intended to maintain direct control of national security affairs, and any National Security Council the Congress wanted to establish would operate within his administration purely as an advisory group to be convened and recessed at the president's discretion.\textsuperscript{8} Consequently, Truman rarely attended NSC meetings.\textsuperscript{9} NSC meetings were chaired by the Secretary of State and often, instead of producing coordinated policy, provided a forum for interagency turf battles.\textsuperscript{10} Department Secretaries sought guidance and decisions in private follow-up meetings with the President.

With the outbreak of the Korean War in 1950, President Truman suddenly found the NSC's function of bringing together senior policymakers to be useful for his own decision-making process.\textsuperscript{11} He began convening regular meetings to develop, discuss, and coordinate policy related to the war. Truman's increased use of the NSC system brought about procedures that have endured to the present day, including interagency committees with responsibilities for specific regional and functional areas, analysis and development of policy options, and recommendations for Presidential decisions.\textsuperscript{12}

The NSC and its staff grew in importance, size, and responsibilities with the election of Dwight D. Eisenhower. President Eisenhower's experience with a military staff system led him to establish an elaborate interagency structure centered on a Planning Board to coordinate policy development, and an Operations Coordinating Board for monitoring the implementation of policies.\textsuperscript{13} Eisenhower also created, in 1953, the post of Special Assistant to the President
for National Security Affairs, now commonly called the National Security Advisor.\textsuperscript{14}

President Kennedy was uncomfortable with the extensive staff and committee system of the Eisenhower presidency and adopted a system where he talked directly with assistant secretaries or others in various agencies, as well as utilizing a small staff of hand-picked experts in the White House.\textsuperscript{15} Under Kennedy, there were only 12 substantive experts on the NSC staff.\textsuperscript{16} Kennedy also was responsible for converting the bowling alley in the basement of the White House West Wing into a Situation Room, where around-the-clock communications are maintained with all national security agencies, U.S. embassies, and military command posts.\textsuperscript{17}

Sharing Kennedy's affinity for more personalized access and control over his advisory system, President Johnson continued with an informal advisory NSC system relying upon the National Security Advisor, a small NSC staff, ad hoc groups, and trusted friends. Johnson instituted a "Tuesday Lunch" policy discussion group that included the Secretaries of State and Defense, CIA Director, and Chairman of the Joint Chiefs of Staff.\textsuperscript{18} Later administrations have found similar weekly breakfasts or lunches among principals to be useful for exploring and coordinating policy issues.

Centralized control of the interagency national security process, and domination of the development and execution of foreign policy by the White House staff reached its zenith under Presidents Nixon and Ford. President Nixon wanted to be certain that the White House fully controlled foreign policy. Henry Kissinger's expanded NSC staff (80 professionals) concentrated on acquiring analytical information from the departments and then refining it for the National Security Advisor. Kissinger then crafted his own written recommendations for President Nixon. The system reflected the President's preference for detailed written assessments rather than group deliberations. This system also reflected Kissinger's dominating personality, as well as his bureaucratic maneuverings to establish the NSC staff as the preeminent national security/foreign policy group in the administration.\textsuperscript{19} Often, Secretary of State Rogers was not even consulted about major foreign policy decisions.\textsuperscript{20} Kissinger's roles in representing Nixon for opening relations with the PRC and negotiating the Vietnam War's Paris Peace Talks are illustrative of the extraordinary operational authority the National Security Advisor received from the President for both policy-making and implementation.

After Richard Nixon's resignation, President Ford inherited the final national security configuration of the Nixon era which found Henry Kissinger serving both as National Security Advisor and as the Secretary of State. Recognizing the pitfalls of vesting too much authority in one individual, Ford appointed Lieutenant General Brent Scowcroft (USAF) as National Security Advisor. As Secretary of State, Kissinger maintained his role as chief foreign
policy advisor to the president, and Scowcroft coordinated analyses and policy options between the executive branch departments and agencies.\textsuperscript{21}

President Carter came into office wanting more diversity in the policy options coming to the president and greater balance in the contributions of department principals to ensure that he was presented with the best policy options available from across his national security system. The interagency process initially was structured to allow for a more prominent role for the State Department. Moreover, Carter’s concerns about foreign policy being overly dominated by a single individual (as it had been by Kissinger) led him to appoint a National Security Advisor (Zbigniew Brzezinski) who was independent and able to provide alternative judgments to those he received from the State Department.\textsuperscript{22} As the administration progressed, Brzezinski increasingly acted as public advocate on policy issues rather than playing a more restricted role as policy broker and coordinator. Brzezinski’s public discourses often led to tensions and disagreements over policy and roles between the NSC staff, State, and other departments.\textsuperscript{23}

The Reagan administration desired a more collegial approach to decision-making and sought to avoid public disagreements among the principal advisors over policy options. The National Security Advisor was downgraded from taking a leading policy development role; now reporting to the Chief of Staff to the President, who exercised a coordinating role in the White House. Collegiality among powerful department heads was not successfully maintained, however, and conflicts became public, especially between the Departments of State and Defense. As a result of this chaotic situation, the Reagan administration has the distinction of having the most National Security Advisors (six individuals), each serving one- or two-year terms. The NSC staff also emerged as an independent actor, not only in formulating policy, but also in implementation. These operational activities resulted in the Iran-Contra affair that was investigated both by the U.S. Congress and a presidential commission.\textsuperscript{24} In 1987, the Tower Commission and congressional investigations determined that the NSC staff deviated from its policy coordination role into policymaking and operational implementation. Both investigations concluded that the mistakes of Iran-Contra were the result of inappropriate decisions by managers and individuals, not flaws in the structure or recommended functions of the national security system.\textsuperscript{25}

Having served eight years as Vice President and participated regularly in deliberations of the Reagan administration, President George H.W. Bush came into office with definite ideas as to how the national security policy process should be organized. First, he appointed Lieutenant General (Ret.) Brent Scowcroft, recognized for his bureaucratic skills and collegial personality, to another tour as the National Security Advisor. President Bush reorganized the NSC system to include a Principals Committee, Deputies Committee, and eight Policy Coordinating Committees, and sought (not always successfully) to establish a collegial system in which the NSC acted as a broker and coordinator
of policy across the Executive Branch. The basic structural organization of interagency working groups, department deputies, and department principals organized in the George H.W. Bush administration has been retained for every succeeding presidential administration.

Like its predecessors, the Clinton administration sought to emphasize a collegial approach within the interagency, but differences over policy recommendations between the NSC staff and the cabinet departments sometimes produced tensions and turf battles. Weekly lunches involving the Secretaries of State and Defense and the National Security Advisor were used by the Clinton administration as a regular senior policy forum for exploring and coordinating issues. The biggest change in the Clinton administration was the emphasis on economics as an element of U.S. national security. The NSC membership was expanded to include the Secretary of the Treasury and the Assistant to the President for Economic Policy, who was head of a National Economic Council (NEC) created by Clinton. The NEC was established to deal with foreign and domestic economic issues in much the same way as the NSC coordinated diplomatic and security issues and some individuals served simultaneously on both the NSC and NEC staffs.

The George W. Bush administration’s NSPD-1 defined the duties of the NSC system to “coordinate executive departments and agencies in the effective development and implementation of ... national security policies.” However, the advent of the terrorist attacks of September 11, 2001 resulted in numerous changes to the original intentions for the Bush administration in the conduct of national security affairs. Most significant among these was the creation of new executive branch organizations related to national security affairs. One of the major findings of both the National Commission on Terrorist Attacks Upon the United States (more commonly known as the 9/11 Commission, and the congressional Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001 (or ‘JICATAS911”) was that there were significant signals of a looming terrorist attack in different parts of the intelligence community, but information and analysis sharing and synthesis was inadequate. One result of these findings was the creation of the Office of the Director of National Intelligence to oversee and direct the implementation of the U.S. National Intelligence Program and act as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. More information on the ODNI and its role is contained in the section of this report on the U.S. intelligence community.

Other major U.S. government organizational structures created during the aftermath of 9/11 were the Homeland Security Council (HSC) and the Department of Homeland Security (DHS). These institutions brought new organizational responsibilities and perspectives to the consideration of national security affairs (both are discussed in detail later in this report). The increased
concern with domestic as well as foreign terrorist threats raised a range of new policy issues including debates over what constitutes "national" versus "homeland" security, separate and overlapping staff responsibilities (as reflected in the number of officials who were members both of the NSC and HSC), and the involvement of state and local governments as considerations in national policy making. National security policy development and coordination was heavily influenced by the Global War on Terrorism, Operation Enduring Freedom, Operation Iraqi Freedom, and by the significant concentration of operational imperatives and resources in the Department of Defense and U.S. Central Command.

The period following the September 11 terrorist attacks brought both temporary operational changes to policy processes, and several organizational changes to the structure of the NSC staff. In the immediate aftermath of the September 11 attacks and subsequent interventions in Afghanistan and Iraq, much of the policy development and decision-making for national security affairs was conducted at the NSC and PC level. Organizational changes in the NSC staff structure included the establishment of the Office for Combating Terrorism headed by a new Deputy Assistant to the President/Deputy National Security Advisor for Combating Terrorism and Deputy Assistants to the President/Deputy National Security Advisors (DAP/DNSA) for Strategic Communication and Global Outreach, and Global Democracy Strategy. Moreover, as the interventions in Iraq and Afghanistan extended into long term Stabilization, Security, Transition and Reconstruction (SSTR) operations, the NSC during the second term of the Bush administration found that it needed to adapt new structures to respond to immediate operational issues requiring high level guidance; political, economic and SSTR concerns; longer term policy planning and consideration of strategic interests; as well as facilitate interagency coordination.

These major, long term interventions during the Bush administration also saw the addition to the NSC of the positions of Special Advisor for Strategic Planning and Institutional Reform, and Special Advisor for Policy Implementation/Execution in 2005. Other changes including elevating the NSC Directorate for Southwest Asia in 2005 to the level of Assistant to the President and Deputy National Security Advisor for Iraq and Afghanistan with sub-directorates for Afghanistan and Iraq, and then in May 2007 expanding the responsibilities for this position to coordinating activities across the Executive Branch to support operational commanders and other U.S. government officials in Iraq and Afghanistan. In particular, this individual reported directly to the president and had the authority to coordinate strategy and policy with department and agency officials up to the level of Cabinet secretaries, as well as solicit information and resources, "identify and remedy" day to day problems, and execute policies and strategies identified by the President.
NSC ORGANIZATION

The National Security Council is the principal forum for consideration of national security policy issues requiring Presidential determination. It is chaired by the President and is called into session at the President's discretion. Its statutory members are the President, Vice President, and the Secretaries of State, Defense and Energy. The Chairman of the Joint Chiefs of Staff is the statutory military advisor to the Council, and the Director of National Intelligence is the intelligence advisor. The National Security Advisor is not a statutory member, but traditionally is responsible for determining the agenda in consultation with the other regular attendees of the NSC, ensuring that the necessary papers are prepared, recording NSC deliberations, and disseminating Presidential decisions. However, the authorities and responsibilities of National Security Advisor, as well as other members of the President's national security team, often have varied significantly from one administration to another.

Although there has been relative stability in the statutory membership of the NSC since its inception, and in the supporting staff structures since the administration of President George H.W. Bush, one fundamental principle underlies the actual operation of the national security structures of all Presidents: the operation of the national security policy process is the result of what the President decides. Those who wish to understand the operations of the NSC and its NSS staff must recognize that regardless of organizational charts or procedural memos produced by each administration, the actual processes are shaped by what the POTUS wants; the authorities he delegates to the various principals, staffs, and organizations; and how his staff conducts its business according their judgments about what the President most needs in terms of policy development, implementation and decision support. As such, formal lines of authority may be over-ridden or circumvented by informal authorities or relationships utilized by the President and/or his senior staff.

In practice, Presidential administrations tend to be unconcerned with whether the membership of a meeting constitutes an "official NSC" meeting, or whether all statutory, designated, or invited members are actually present. The participants in meetings at all levels are dictated by the requirements of the policy issue(s) at hand. If the President (or other principal) is needed, he will be present. If not, then his limited discretionary time will not be diverted to attending a meeting just so all the "members" will be recorded as present. For example, although the Secretary of Energy is a statutory NSC member, he is unlikely to attend unless energy or nuclear development or security issues are on the agenda.

In addition to the statutory members, each president traditionally designates other NSC members, regular attendees, invited attendees, and topic area invitees. According to the Obama administration's Presidential Policy Directive-1, which sets out the organization of the National Security Council
system, in addition to the statutory members indicated above, President Obama has directed that the "membership" of the NSC will include: the Secretary of the Treasury, the Attorney General, the Secretary of Homeland Security, the Representative of the United States of America to the United Nations, the Assistant to the President and Chief of Staff (Chief of Staff to the President), and the Assistant to the President for National Security Affairs (National Security Advisor).

Regular attendees include:
- The Director of National Intelligence (as a statutory advisor)
- The Chairman of the Joint Chiefs of Staff (as a statutory advisor)

Regular invited attendees include:
- The Counsel to the President
- The Assistant to the President and Deputy National Security Advisor (also designated to serve as Secretary)

Topic area invitees:
Invitees as required when international economic issues are on the agenda:
- The Secretary of Commerce
- The United States Trade Representative
- The Assistant to the President for Economic Policy
- The Chair of the Council of Economic Advisers.

Regular invitee for homeland security or counter-terrorism issues:
- The Assistant to the President for Homeland Security and Counterterrorism

Regular invitee for science and technology related issues:
- The Director of the Office of Science and Technology Policy

Heads of other executive departments and agencies, as well as other senior officials, also are invited when appropriate.

The National Security Advisor is the President's personal advisor responsible for the daily management of national security affairs, and advises the President on the entirety of national security matters and coordinates the development of interagency policies. Thomas E. Donilon succeeded General James L. Jones as President Obama's NSA in October 2010. The President alone decides national security policy, but the National Security Advisor is responsible for ensuring that the President has all the necessary information, that a full range of policy options have been identified, that the prospects and risks of each option have been evaluated, that legal and funding considerations have been addressed, that potential difficulties in implementation have been identified, and that all NSC principals have been included in the policy development and recommendation process. President Obama has stipulated that his National Security Advisor
preside at NSC meetings in his absence (officially, if the President does not attend, the meeting is a Principals Committee meeting and not an NSC meeting). The National Security Advisor, appointed by the President as a personal aide, is not subject to Congressional confirmation. Thus, any attempt at reviewing the processes or policymaking of the National Security Council and its staff by Congress must be conducted through meetings with the President or other Senate-confirmed principals of the National Security Council.

The professionals who work directly for the President under the National Security Advisor's direction constitute the National Security Staff. President Obama, shortly after taking office, promulgated Presidential Policy Directive-1 (PPD-1, see Appendix C for a list of PPDs and President Study Directives-PSDs), "Organization of the National Security Council System," which established the procedures for assisting the President in carrying out his responsibilities in the area of national security. He also merged the Homeland Security Council Staff and the National Security Council Staff into a single National Security Staff. Under PPD-1, the NSS is charged with running a proactive and rigorous interagency policy process, consisting of Interagency Policy Committees (IPC), chaired by a Senior Director and consisting primarily of interagency Assistant Secretaries; Deputies Committees (DCs), chaired by either the Deputy National Security Advisor or the Assistant to the President for Homeland Security and Counterterrorism and consisting primarily of interagency Deputy Secretaries; and Principals Committees (PCs), chaired by either the National Security Advisor or, at times, the Assistant to the President for Homeland Security and Counterterrorism and consisting primarily of interagency Secretaries. The IPCs, DC, and PCs can all make decisions, but must do so by consensus of its interagency members. The chair, including the NSA, cannot make decisions or "break ties."

NSS staff members handling substantive issues include political appointees (frequently experts from think tanks and academia), senior professionals on detail from Executive Branch departments, and military officers. The expertise of career Foreign Service Officers in foreign affairs, for example, often means that the senior positions of the NSS regional directorates are assigned to State Department personnel. This staff (see Appendix D) conducts the day-to-day management of national security affairs for the White House and currently numbers approximately 320, with around 175 policy positions and the remainder support positions (including the White House Situation Room staffed by approximately 35 watch officers and 35 technical/communications staffers). However, the NSC and its staff also are able to rely on a network of former NSC members, staffers, and other trusted policy experts, if needed, when reviewing policy issues.

President Obama has conducted formal NSC meetings on a regular basis throughout his administration, but has emphasized the composition of meetings according to the topics under consideration and the needs of the President rather
than concerns with formally established "National Security Council" meetings. Press statements from the Obama White House often mention the President's meetings with his "national security team" rather than the formal NSC. Although the Obama administration regularly utilizes the technological upgrades to the White House Situation Room implemented during 2006-2007, President Obama prefers to hold NSC meetings in person, and most PC meetings are face-to-face. Use of the Secure Video-Teleconference Service (or SVTS—pronounced “civts”) is used when the President or other principals travel, or for Deputies Committee, Interagency Policy Committee meetings or other inter-departmental discussions.

The most senior interagency group is the Principals Committee (NSC/PC). The PC for all practical purposes is the membership of the NSC without the President and Vice President. The PC is called into session and chaired by the National Security Advisor. In addition to the National Security Advisor, the other principal members of the PC are the Secretaries of State, Defense, Treasury, Homeland Security, and Energy, the National Security Advisor, the Attorney General, the Director of the Office of Management and Budget, the Representative of the United States of America to the United Nations, the Chief of Staff to the President, the Director of National Intelligence, and Chairman of the Joint Chiefs of Staff.

The Obama administration Principals Committee meets on a regular basis (usually at least weekly) to discuss current and developing national security issues, review and coordinate policy recommendations developed by subordinate interagency groups and affected departments and agencies, and give direction for implementation or follow-up analyses. The Vice President attends PC meetings when issues related to his interests or responsibilities are being considered.

Other key Executive Branch officials may be invited to attend Principals Committee meetings when issues related to their areas of responsibility are discussed. Regularly invited attendees include the White House Chief of Staff, Counsel to the President, and the Assistant to the Vice President for National Security Affairs. Topic area invitees may include the Secretary of Commerce, the United States Trade Representative, and the Assistant to the President for Economic Policy when international economic issues are on the Agenda. Topic area invitees for homeland security or counterterrorism related issues usually include the Assistant to the President for Homeland Security and Counterterrorism (who also serves as the PC chair on homeland security topics). Topic area invitees for science and technology related issues might include the Director of the Office of Science and Technology Policy. Similar to NSC meetings, the heads of other executive departments and agencies, along with additional senior officials, may be invited to PC meetings as appropriate.

Subordinate to the Principals Committee is the Deputies Committee (NSC/DC). As the senior sub-Cabinet interagency forum, the DC is responsible
for directing the work of interagency working groups and ensuring that issues brought before the PC or the NSC have been properly analyzed and prepared for high-level deliberation. President Obama has codified this responsibility for the DC in his Presidential Policy Directive organizing the National Security Council System (PPD-1) by directing that “NSC/DC shall ensure that all papers to be discussed by the NSC or the NSC/PC fully analyze the issues, fairly and adequately set out the facts, consider a full range of views and options, and satisfactorily assess the prospects, risks, and implications of each.”

Historically, the DC is where the bulk of the government’s policy decisions are made in preparation for the PC’s review and the President’s decision. Issues decided above the DC level either are the most sensitive national security decisions, are very contentious within the interagency, or both. In some circumstances (e.g., crisis situations) a significant portion of interagency policy development and coordination may be done at the DC level rather than at lower levels. PPD-1 specifically identifies this responsibility of the DC by directing that “the NSC/DC shall be responsible for day-to-day crisis management.” As such, the DC meets very frequently —usually on a daily basis, and sometimes several times a day.

The DC is composed of the deputy or relevant under secretaries to the cabinet secretaries. The DC is chaired by the Assistant to the President and Deputy National Security Advisor (AP/DNSA) or the Assistant to the President for Homeland Security and Counterterrorism. The regular members of the DC include the Deputy Secretary of State (who in practice sometimes may be represented by the Under Secretary of State for Political Affairs), Under Secretary of the Treasury (who sometimes may be represented by the Under Secretary of the Treasury for International Affairs), Deputy Secretary of Defense (who sometimes may be represented by the Under Secretary of Defense for Policy), Deputy Attorney General, Deputy Secretary of Energy, Deputy Director of the Office of Management and Budget, Deputy to the United States Representative to the United Nations, Deputy Director of National Intelligence (or sometimes the Director of the National Counterterrorism Center if counterterrorism issues are being considered), Vice Chairman of the Joint Chiefs of Staff, and Assistant to the Vice President for National Security Affairs.

Like the PC, other senior executive branch officials may participate in DC meetings when appropriate for the substantive issues on the agenda. The Assistant to the President for Homeland Security and Counterterrorism and Deputy National Security Advisor chairs DC meetings when homeland security or counterterrorism related issues are on the agenda, and attends meetings on other topics as appropriate. Likewise, the Deputy Assistant to the President and Deputy National Security Advisor for International Economics will attend DC meetings when international economic issues are on the agenda and may be directed to chair the meeting at the discretion of the AP/DNSA. PPD-1 also directs that an Associate Director of the Office of Science and Technology Policy
will participate in DC meetings when science and technology related issues are being considered.

Subordinate to the DC are a variety of interagency working groups called Interagency Policy Committees (NSC/IPCs). These interagency committees are composed of substantive experts and senior officials from the departments and agencies represented on the DC. Although bounded by how much control is exerted over policy issues by the PC and DC groups, IPC-type committees historically are the main forum for interagency coordination. These groups conduct the day-to-day interagency analysis, generation of courses of action, policy development, coordination, resource determination, and policy implementation planning. Sometimes events may affect this traditional role, as when crisis situations or other high level national security developments warrant considerable attention by the PC or NSC.

Contingent upon the scope of their responsibilities, some IPCs may meet regularly (weekly or even several times daily in a crisis situation) while others meet only when developments or planning require policy synchronization. They are responsible for managing the development and implementation of national security policies when they involve more than one government agency. IPCs provide policy analysis for consideration by the more senior committees of the NSC system (e.g., the DC and PC) and ensure timely responses to decisions made by the President. The role of each IPC in policy development and implementation has tended to vary from administration to administration according to the amount of authority and responsibility delegated to them by the DC and PC. In the Obama administration, IPCs are expected whenever possible to find consensus before elevating issues to DCs. They are organized around either regional or functional issues.

Regional IPCs normally are headed by Assistant Secretaries of State while functional IPCs are headed by senior department officials or NSS Senior Directors.

The Obama administration has not released an unclassified list of IPCs. However, the IPCs of the new administration can be expected to continue to work on policy issues in most of the same areas as the PCCs that functioned during the George W. Bush administration.

Regional PCCs that functioned during the Bush administration included (the department responsible for chairing the committee is in parentheses):

- Europe and Eurasia (State)
- Western Hemisphere (State and NSC co-chair)
- Mexico/Central America Regional Strategy (State and NSC co-chair)
- East Asia (State)
• South and Central Asia (State)
• Iran (State and NSC co-chair)
• Syria-Lebanon (State and NSC co-chair)
• Africa (State and NSC co-chair)
• Russia (State and NSC co-chair)
• Iraq (NSC)
• Afghanistan (State and NSC co-chair)

Functional PCCs that functioned during the Bush administration included (the department responsible for chairing the committee is in parentheses):

• Arms Control (NSC)
• Biodefense (NSC and HSC)
• Combating Terrorism Information Strategy (NSC)
• Contingency Planning/Crisis Response Group (NSC)
• Counter-Terrorism Security Group (NSC and HSC)
• Defense Strategy, Force Structure, and Planning (DOD)
• Democracy, Human Rights, and International Operations (NSC)
• Detainees (NSC)
• Global Environment (NSC and NEC co-chair)
• HIV-AIDS and Infectious Diseases (State & NSC)
• Information Sharing (NSC and HSC)
• Intelligence and Counterintelligence (NSC)
• Interdiction (NSC)
• International Development and Humanitarian Assistance (State and NSC co-chair)
• International Drug Control Policy (NSC and ONDCP)
• International Finance (Treasury)
• International Organized Crime (NSC)
• Maritime Security (NSC and HSC)
• Proliferation Strategy, Counterproliferation, and Homeland Defense (NSC)
• Reconstruction and Stabilization Operations (State and NSC)
• Records Access and Information Security (NSC)
• Space (NSC)
• Public Diplomacy and Strategic Communications (State)
• Transnational Economic Issues (NSC)
• Weapons of Mass Destruction – Terrorism (WMD-T) (NSC)
• Avian and Pandemic Influenza (NSC and HSC)
• Communication Systems and Cybersecurity (NSC and HSC)
Although IPCs are divided into regional or functional groups, participation is not limited to people with only regional or functional expertise. Regional IPCs may include department or agency members with functional expertise, and functional IPCs are likely to include regional experts. For example, the non-proliferation IPC may include regional experts covering countries involved with proliferation issues, and the Counterterrorism Security Group (or CSG, which meets weekly) includes representatives from the Department of Homeland Security.

The NSC, PC, DC, and IPC entities all are supported by the National Security Staff. The NSS is one of several senior advisory groups or offices organized under the Executive Office of the President (EOP) to advise the President across a range of critical policy areas. Although the councils and offices of the EOP have tended to remain fairly stable across administrations (some components, such as the Council of Economic Advisors is statutory, while others, such as the National Economic Council, have been created by Executive Orders), Presidents often have altered their structures or created new policy advisory or analysis groups as a result of historical events.

**National Security Staff**

The Obama administration believes that “homeland security is indistinguishable from national security” and has been using a single, integrated staff structure to manage both national security and homeland security crises and policy development and implementation. Although President Obama has determined that the Homeland Security Council should be retained as the “principal venue for interagency deliberations on issues that affect the security of the homeland such as terrorism, weapons of mass destruction, natural disasters, and pandemic influenza,” he also determined that the NSC and HSC should be supported by a single “National Security Staff” headed by the National Security Advisor. To ensure proper attention is paid to homeland security and counterterrorism issues at the NSS, day-to-day responsibilities in these areas are assigned to the Assistant to the President for Homeland Security and Counterterrorism/Deputy National Security Advisor (AP/HSCT & DNSA), and his Deputy Assistant to the President for Homeland Security (DAP/HS, see Appendix D).

The Obama administration’s NSS views homeland security issues within a global context and has sought to avoid characterizing security matters as homeland versus international. Responsibilities for “national security” or “homeland security” are derived from the substantive areas of responsibility assigned to each directorate. For example, if homeland security matters arise in a regional directorate, those staffers are expected to be responsible for coordinating with the AP/HSCT, the DHS, the Department of State, or other appropriate agencies for the development of policy analysis and recommendations to the DC, PC, or the President.
As revealed in its organizational structure, the NSS handles a wide range of substantive national security issues for President Obama (see Appendix D). Two specific areas that continue to receive considerable NSS, congressional, and domestic attention are Iraq and Afghanistan. These two areas illustrate the extent to which NSS structures and functions may change and adapt to seek the most effective organizational processes to handle complex national security problems. For example, U.S. policy for Iraq is handled in the Gulf sub-Directorate of the Central Region Directorate of the NSS. The Iraq Policy and Operations Group (IPOG) established during the first term of the George W. Bush administration was dissolved in August 2011 and its remaining functions relegated back to IPC and other departmental and interagency working groups.

**Homeland Security Council**

The Homeland Security Council (HSC) was established on October 8, 2001 in response to the terrorist attacks of September 11, 2001, and serves as the mechanism for ensuring coordination of homeland security-related activities of executive departments and agencies and effective development and implementation of homeland security policies. President Obama has stated that he views the HSC as his “principal venue for interagency deliberations on issues that affect the security of the homeland such as terrorism, weapons of mass destruction, natural disasters, and pandemic influenza.” It also serves as the President’s principal forum for reviewing homeland security policy matters with his senior national security advisors and cabinet officials.

The Obama administration has retained the membership of the HSC as specified in HSPD-1. The members of the HSC include the President, the Vice President, the Secretary of Homeland Security, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, the Secretary of Transportation, the Director of the Federal Bureau of Investigation, the Director of National Intelligence, the Director of the Office of Management and Budget, the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT), the Chief of Staff to the President, and the Chief of Staff to the Vice President. The Assistant to the President for National Security Affairs and the Counsel to the President are invited to attend all meetings of the HSC. The Secretary of State and the Chairman of the Joint Chiefs of Staff (as the statutory principal military adviser to the HSC) have regularly attended HSC meetings during the Bush administration, as well as the Secretary of Agriculture, Secretary of the Interior, Secretary of Energy, Secretary of Labor, Secretary of Commerce, Secretary of Veterans Affairs, Administrator of the Environmental Protection Agency, Assistant to the President for Economic Policy, and Assistant to the President for Domestic Policy who are invited to attend meetings pertaining to their responsibilities. The heads of other executive departments and agencies and other senior officials are invited to attend Council meetings when appropriate.
The HSC meets with the President at his direction and, during the Obama administration, has met less frequently than the NSC. This pattern is the result of President Obama's emphasis on bringing together principals who need to be consulted on various policy issues (vice convening a formal HSC meeting), as well as the overlap between the membership of the NSC and its PC and the HSC and its PC. At the President's direction, the APHS/CT may preside at HSC meetings when the POTUS is absent. The APHS/CT also is responsible for determining the agenda, ensuring that necessary papers are prepared, and recording Council actions and Presidential decisions. Like the National Security Advisor in matters of national security, the APHS/CT serves as the President's key homeland security and counterterrorism advisor in the White House.

The HSC Principals Committee (HSC/PC) and Deputies Committee (HSC/DC) both continue to operate under the Obama administration's NSS reorganization. The Principals Committee of the Homeland Security Council is organized as the senior interagency forum for homeland security issues. With the merging of the NSC and HSC staffs (into the National Security Staff), more homeland security and counterterrorism issues are handled by the NSA, the APHS/CT, Principals and other appropriate advisors, resulting in less need for formal HSC/PC meetings. However, the HSC/PC meets whenever necessary, and individual PC members meet on regular basis with each other to discuss developments and policy issues. Regular members of the HSC/PC include the Vice President, Secretary of Homeland Security, Secretary of the Treasury, Secretary of Defense, Attorney General, Secretary of Health and Human Services, Secretary of Transportation, Director of the Federal Bureau of Investigation, Director of National Intelligence, Director of the Office of Management and Budget, APHS/CT, Chief of Staff to the President, and Chief of Staff to the Vice President. The meetings are chaired by the APHS/CT or another senior staff member, and the National Security Advisor and the Counsel to the President are invited to attend all meetings. Other key Executive Branch officials may be called to attend HSC/Principals Committee meetings when issues related to their areas of responsibility are discussed. These invitees may include the Secretaries of State, Interior, Commerce, Agriculture, Labor, Energy, Veterans Affairs, and the Administrator of the Environmental Protection Agency.

A comparison of NSC and HSC organizations reveals that all 11 members (or statutory advisors or frequent substantive invitees) of the NSC are official HSC members (the President, Vice President, Secretary of Defense, Attorney General, Director of National Intelligence,) or invited participants (the Secretaries of State and Energy, the Chairman of the Joint Chiefs of Staff, the Chief of Staff to the President, the Assistant to the President for National Security Affairs, White House Counsel, Assistant to the President for Economic Policy and Director of the Office of Management and Budget) to the HSC. As noted above, the Obama administration has tended to focus on determining participants in policy meetings according to the substance of the meeting and the appropriateness of the participants, and has been less concerned about whether
the membership of the group constitutes a formal NSC, HSC, or PC meeting. Meetings among principals, the President, and staff occur on a regular basis each week to deal with events and the development of policy.

The HSC system also has a Deputies Committee (HSC/DC) and Interagency Policy Committees (IPCs). The role of the HSC/DC is to ensure that matters brought before the HSC or HSC/PC have been properly analyzed, reviewed by key interagency stakeholders, and prepared for action. The HSC/DC meets on a regular basis to oversee homeland security issues and manage breaking incidents. The regular members of the HSC/DC include the Deputy Secretary of Homeland Security, Deputy Secretary of the Treasury, Deputy Secretary of Defense, Deputy Attorney General, Deputy Secretary of Transportation, Deputy Secretary of Health and Human Services, Deputy Director of National Intelligence, and Deputy Directors of the Office of Management and Budget, and the FBI. The HSC/DC meetings are chaired by the Deputy Assistant to the President for Homeland Security. The Deputy National Security Advisor, Deputy Chief of Staff to the President, and Deputy Chief of Staff to the Vice President are invited to attend all meetings. Other officials who may be invited to attend HSC/DC meetings when issues pertaining to their departmental responsibilities or areas of expertise are involved include Deputy Secretaries of State, Interior, Commerce, Agriculture, Labor, Energy, Veterans Affairs, and the Environmental Protection Agency. Given the wide range, and often overlapping interests of the HSC and the NSC and their various sub-committees, organizers try to avoid encroaching upon already busy schedules. Meeting schedules and topics are widely disseminated in advance across the interagency to allow invitees to determine whether departmental interests are involved, and whether their presence is needed.

Because the HSC remains as a separate policy advisory body, the Obama administration has retained a variety of Interagency Policy Coordination Committees (IPCs) subordinate to the HSC/DC. These interagency committees are composed of Assistant Secretary-level officials from the departments and agencies represented on the DC. Each department or agency representative is designated by his or her department or agency, and is expected to be able to speak on behalf of the department or agency. HSC IPCs are the workhorses of the HSC policy development and coordination process, typically providing the first serious, broad interagency review and discussion of proposals or initiatives; they also provide policy analysis and recommendations for the more senior committees of the HSC system. Most IPCs meet on a weekly basis.

The Obama administration has not released an unclassified list of HSC IPCs. However, many will continue the work of the HSC PCCs that functioned during the George W. Bush administration. Bush HSC PCCs included (all chaired by HSC Special Assistants to the President):

- Biodefense
• Border and Transportation Security  
• Communications Systems and Cybersecurity (CSC, administered jointly with NSC)  
• Continuity  
• Critical Infrastructure Protection  
• Domestic Nuclear Defense  
• Domestic Readiness  
• Information Sharing (administered jointly with NSC)  
• Maritime Security (administered jointly with NSC)  
• National Security Professional Development

**National Economic Council**

One notable example of an advisory office established in response to historical developments and increasing influence on U.S. national interests is that of the National Economic Council (NEC). Historically, international economic issues were handled by the NSC staff and supported by the President's Council of Economic Advisors (a small office established in 1946 to provide the President with objective economic analysis and advice). The increasing complexity of macro-economic issues, however, and the extent to which national interests progressively involved economic policy led to the creation of the National Economic Council in 1993 by President Clinton and the appointment of an Assistant to the President for Economic Policy. The NEC advises the President on matters related to global economic policy. By Executive Order, the NEC has four principal functions: to coordinate policy-making for domestic and international economic issues; to coordinate economic policy advice for the President; to ensure that policy decisions and programs are consistent with the President's economic goals; and to monitor implementation of the President's economic policy agenda.\(^{45}\)

The purview of the NEC extends to policy matters affecting the various sectors of the nation's economy, as well as to the overall strength of the U.S. and global economies. Therefore, in general, members of the NEC are the department and agency heads whose policy jurisdictions affect the nation's economy. The NEC staff is composed of policy specialists whose expertise pertains to the Council's specific areas of decision-making. In the past there have been two Assistants to the President whose responsibilities are divided between domestic and international economic issues. Currently there is one Assistant to the President for Economic Policy (who also serves as the Director of National Economic Council) and one Deputy Assistant to the President (and Deputy National Security Advisor) for International Economics. The Deputy Assistant for International Economics reports both to the National Security Advisor and the NEC Director. The NEC staff also is comprised of two other Deputy Assistants to the President and several Special Assistants to the President who report to the Director on economic policy issues related to fiscal

23
255
policy, energy, financial markets, health care, and labor. Several NSS staff members, who report directly to the Deputy National Security Advisor, also support and coordinate with the NEC Director.

Increasingly from the time of the Clinton administration, economic issues are a major concern in the overall national security of the United States. In many foreign policy areas, economic issues have become equally or more important than traditional military issues—as in the case of China. Also increasingly, international and domestic policy issues and their implications for the well-being of the U.S. are seen to overlap. As a result, there is increased coordination and integration between the NSS and NEC staffs across the spectrum of economic policy issues.

**NSC POLICY PROCESS**

The process of producing national security policies is determined by the organizational structure of the system approved by the President, the National Security Advisor’s overall management of the system, and the performance of key individuals responsible for foreign policy and other national security issues across the executive branch. Perhaps the most thorough analysis and critical assessment of the policy processes for national security was conducted by the Project on National Security Reform, and reported in its “findings” report of July 2008.\(^{46}\) Headed by a board of senior, experienced former government officials, the project evaluated the national security policy development and execution process in various administrations and identified the organizational strengths and weaknesses of those processes. One finding of the report was that the working relationships of the “different parts of the national security system” always reflected “the managerial style of the president.” Furthermore, “(d)ifferent presidents rearranged these relationships frequently. However, only infrequently would they seek to change the bureaucracies themselves or significantly alter the outputs these bureaucracies were expected to produce.”\(^{47}\)

Thus, the basic organizational structures used by each presidential administration since that of George H.W. Bush have tended to be remarkably similar. Nevertheless, no matter how similar various administration organizational charts may be, or however the National Security Advisor and the staff want to organize meetings, procedures, or prepare reports, the actual process is shaped by the President’s management style and what structures and processes the president desires and supports. It is the President’s preferences for using (or excluding) different subordinates in his decision making process, what responsibilities, authorities, and access he allocates to his staff at the White House or various executive branch departments and agencies, and (perhaps most importantly) how he refines the process based upon the successes or failures of his system to produce satisfactory results in foreign policy and other
national security affairs that yield the actual day-to-day "policy process" of his administration. As such, particularly as an administration's term proceeds, formal lines of authority may be over-ridden or circumvented by informal authorities or relationships utilized by the President and/or his senior staff.

The National Security Council is the President's principal forum for considering national security and foreign policy matters with his senior national security advisors and cabinet officials. The National Security Act of 1947 directs that the function of the NSC "shall be to advise the President with respect to the integration of domestic, foreign, and military policies related to the national security so as to enable the military services and the other departments and agencies of the government to cooperate more effectively in matters involving the national security," as well as to perform "other functions the President may direct for the purpose of more effectively coordinating the policies and functions of the departments and agencies of the government relating to the national security." The NSC has the responsibility to "assess and appraise the objectives, commitments, and risks of the United States" and to "consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security." Ensuring the continuity of this important organization in the current administration is reflected in President Obama's Presidential Policy Directive #1 which directs that "the NSC shall advise and assist me in integrating all aspects of national security policy as it affects the United States -- domestic, foreign, military, intelligence, and economic (in conjunction with the National Economic Council). Along with its subordinate committees, the NSC shall be my principal means for coordinating executive departments and agencies in the development and implementation of national security policy."

When the president makes a policy decision he usually will transmit the information verbally to the relevant cabinet secretaries, the National Security Advisor, or other appropriate officials. Frequently, this takes place at formal NSC meetings. At times, he will wish to ensure that there is clear understanding of policy objectives and requirements of the initial decision, and he will issue a formal decision document (which may be classified or unclassified) stating the policy in order to communicate the specifics of the decision to affected government departments and agencies, or to the general public. The current Obama administration calls these formal policy decisions Presidential Policy Directives (PPDs). See Appendix A for the titles used in previous administrations.

The National Security Advisor and the Policy Process

Presidents rely heavily upon their National Security Advisor (NSA, whose formal title is Assistant to the President for National Security Affairs) to undertake a number of specific roles to support them in the management of national
security affairs. Because the National Security Advisor is a personal aide to the President, this person must enjoy the President's full trust and confidence. The 1987 report by the Tower Commission on the operation of the NSC staff identified a number of specific roles for National Security Advisors that have evolved and proven beneficial to the President in the effective management of national security affairs.  

- He is an "honest broker" for the NSC process. He assures that issues are clearly presented to the President; that all reasonable options, together with an analysis of their disadvantages and risks, are brought to his attention; and that the views of the President's other principal advisors are accurately conveyed.
- He provides advice from the President's vantage point, unalloyed by institutional responsibilities and biases. Unlike the Secretaries of State or Defense, who have substantial organizations for which they are responsible, the President is the National Security Advisor's only constituency.
- He monitors the actions taken by the executive departments in implementing the President's national security policies. He questions whether these actions are consistent with Presidential decisions and whether, over time, the underlying policies continue to serve U.S. interests.
- He assumes a special role in crisis management. The rapid pace of developments during crises often draws the National Security Advisor into an even more active role of advising the President on the implications for national security of unfolding events. He fulfills the need for prompt and coordinated action under Presidential control (often with secrecy being essential) and in communicating Presidential needs and directives to the departments and agencies of the Executive Branch.
- He reaches out for new ideas and initiatives that will give substance to broad Presidential objectives for national security.
- He keeps the President informed about international events and developments in the Congress and the Executive Branch that affect the President's policies and priorities.

The emphasis placed upon these various roles as they are described in the Tower Commission report varies from administration to administration according to the President's preferences for managing national security affairs, the National Security Advisor's interpretation of his or her role, and the personalities and styles of the various members of the Principals Committee and other policymaking bodies.

The national security policy process during the first years of the Obama administration mirrored that of previous administrations in the challenges of having the capability to immediately advise the President on a wide range of national security matters while establishing its staffing, procedures, and
processes. No new administration comes into office with a fully staffed, unified national security team. The National Security Advisor must draw upon and integrate experts and advisors from the presidential campaign retinue, professionals from previous administrations with national security experience, academic and think tank experts, and, finally, senior career employees from across the executive branch with deep experience in national security affairs.

In general, the National Security Advisor’s (NSA) primary roles are to advise the President, advance the President’s national security policy agenda, and oversee the effective operation of the interagency system. The NSA must be able to manage the process of integrating information and policy considerations affecting national interests across the spectrum of government agencies and instruments of power and foreign policy, prioritizing their strategic importance, and synthesizing them into concise issues and options for the President’s consideration. Moreover, the NSA must bring to the President not only information he wants to see, but also information he needs to see—and in a form compatible with the President’s decision-making and management style. For example, President George W. Bush preferred to make the final decision on policy recommendations that reflected a consensus of his advisors. As such, NSAs Rice and Hadley sought to hammer out a general agreement among Principals and departments before bringing a decision paper with a recommended policy to President Bush for a final decision. President Obama, on the other hand, prefers not to have recommended positions brought to him for a yes or no decision. Instead, he favors a slate of options on policy issues with detailed assessments of the pros and cons for each option. If brought a consensus position by his policy advisors, President Obama also expects to see a full analysis of any significant dissenting positions on the policy area under consideration.

The NSA should bring to the President only those issues that have been vetted through the interagency system so that he can benefit from the counsel of those departments with concomitant responsibilities and authorities. The NSA also must ensure that, given demands upon the President’s time from such a wide variety of policy issues and political constituencies, the President only has to deal with those problems that require his level of involvement. This is a delicate management problem to not usurp the President’s authority on “lower level” issues, while, at the same time, not consume his limited time on issues that others have been delegated the authority to decide.

Protecting the President’s time involves not only concisely and effectively presenting issues to the President, but also managing the constant demands of visiting dignitaries and modern telecommunications that allow foreign governments, U.S. Ambassadors, military commanders, and other officials throughout the world the capability to communicate directly with the White House. Increasingly, the ability for foreign leaders and others to converse directly means the NSA must manage the President’s direct communications and
act as a gatekeeper for the President to determine who warrants access to directly discuss national security matters.\textsuperscript{53}

On occasion, protecting the President's time requires the NSA to meet with foreign officials to deliver or receive messages, or discuss U.S. policy (as when NSA Donilon met with Israeli Minister of Defense Barak over security cooperation and developments in the Middle East in February 2011, with members of the Libyan Transitional National Council in May 2011, and with UN Secretary-General Ban Ki-moon over Middle East events and the humanitarian emergency in the Horn of Africa in July 2011).\textsuperscript{54} The Tower Commission strongly cautioned that neither the National Security Advisor nor the NSC staff should be engaged in operations, or the direct implementation of policy, as happened during the Iran-Contra affair. Nevertheless, although the Department of State clearly has the responsibility for dealing with foreign officials and implementing foreign policy, the NSA may act as the President's emissary to the extent that the President wishes to use the National Security Advisor in this manner—although this role has been utilized sparingly in recent administrations.

The National Security Advisor also has responsibilities beyond national security affairs that affect the President's domestic political standing. This involves the NSA's dealings with Congress and the media. The NSA must work alongside other executive branch officials to build trust with Congress in order to facilitate cooperation between the branches to achieve the administration's national security objectives. Moreover, the NSA must avoid, if possible, any appearance of national security decisions being driven by domestic politics (e.g., emphasizing international crises to divert attention from a domestic political problem), both because national security affairs should be dealt with on their own merits, and because of the need to build bi-partisan consensus on foreign policy issues. As such, one additional responsibility of the NSA is insulating the NSS staff from any political pressure—either from other components of the White House staff responsible for domestic political affairs or from political interests outside the White House. This can be a difficult mission because national security priorities (and, in particular, those dealing with homeland security issues) often are influenced by domestic politics or have domestic implications. Consequently, the NSA must focus on advising the President about broader national security problems while being mindful of domestic political factors that may influence the acceptability of policy options.

The National Security Advisor's dealings with the media are complicated because while the Secretary of State is primarily responsible for the overall management and explanation of foreign policy, the NSA often acts as an "explicator" of policy to the media. The NSA must balance secrecy requirements with the public's right to know, and the unrelenting pressure from the media for information on a daily basis. Secrets are difficult to maintain in a democracy with a massive bureaucracy and a free press. According to former NSC/NSS staffers, news reporting and analysis generally lags policy decisions by 3-4 days
and is about 60-80% accurate, depending upon the news operation and its familiarity with the issues being covered.

Thus, to be effective, the National Security Advisor must have the trust of the President, the principals of the departments and agencies involved in national security matters, substantive experts in the bureaucracy, numerous foreign leaders and their ministries, members of both parties in the Congress, and the news media. He, or she, must be able to manage this series of complex interrelationships and promote cooperation rather than competition among the various stakeholders. In an increasingly complex, multi-dimensional policy world still possessing strategic threats, the NSA must effectively administer advice and access to the President to enable him to effectively do this part of his job.

A list of the individuals who have served as the National Security Advisor, and the dates they served, is attached at Appendix B.

The National Security Staff and the Policy Process

Like the National Security Advisor, the roles and missions undertaken by the National Security Staff have evolved over time. Variations from one administration to another are due largely to presidential preferences as to specific NSS roles, organizational and management preferences of the National Security Advisor, and changes brought about through the necessity of responding to crises or complex national security problems. One of the most significant examples was the decision on May 26, 2009 by President Obama to reorganize the previous NSC and Homeland Security Council staffs into a single “National Security Staff.”55 Although this reorganization did not substantially affect the normal practices of crisis response, policy development, and implementation oversight, it did have the effect of fully integrating international, transnational and homeland security matters, and placing all policy matters under a single organizational chain of command.

Although the National Security Staff (NSS) frequently plays a key role in policy development and recommendations because of their direct relationship with the President, a close working relationship between the President and his cabinet secretaries may result in those departments dominating the development and implementation of national security policy. Alternatively, greater dependence by the President on the National Security Advisor and interagency rivalries sometimes can lead to a more active role in initiating and guiding policy for the NSS. Historical events also can limit or expand the roles taken on by the NSS. For example, the establishment of the National Economic Council in 1993 resulted from the increasing importance and complexity of economic issues in national security policy following the collapse of the Soviet Union and the growth of fledgling market economics in former communist countries. Likewise, the
terrorist attacks of September 11, 2001 increased the involvement of the NSC staff in counterterrorism policymaking for both domestic and international venues, and the political and military complexities of U.S. actions in Afghanistan and Iraq have emphasized the roles of DOD and the State Department in policy development and implementation.

Some of the responsibilities of the (previous) NSC staff and current NSS that have evolved over time as a result of bureaucratic dynamics and historical developments include.\textsuperscript{56}

- Coordination of the interagency policy process and policy implementation follow-up.
- Articulation of the President’s policies to other departments and, at times, to the U.S. public (through the National Security Advisor).
- Liaison with foreign governments.
- Support to the President during telephone conversations with foreign leaders.
- Support for negotiations in Presidential summits.\textsuperscript{57}
- Coordination of summit meetings and overseas travel by the President.
- Direct support to the President in crisis management.

The development of coordinated interagency strategic national security policy is both a priority and a challenge for the President and his National Security Staff. All components of the NSS are expected to work closely with other executive branch departments and agencies on a continuing basis. For the Obama NSS, the newly organized Strategic Planning Directorate, in particular, works across directorates to provide strategic oversight for the policy process. The Strategic Planning Directorate currently performs five core functions: 1) support on the administration’s top national security priorities, particularly those that require broad development of policy guidance; 2) assistance on urgent crises; 3) supporting the President’s engagement and outreach to key allies, partners and the strategic community; 4) ensuring strategic and contingency planning conforms to Presidential guidance; and 5) assisting the National Security Advisor with special projects.

The wide-ranging duties and activities of the NSS result from the fact that the National Security Advisor and the NSS work directly for the President. Although the Secretaries of State and Defense are cabinet level officials who belong to the formal National Security Council, they have no authority over the NSS. To the extent that the National Security Advisor and his/her staff take on functions seen as the prerogative of departments or agencies, tensions and turf battles can develop that may affect the ability of an administration to develop and coordinate policy. Moreover, whenever NSS takes on operational roles it raises concerns that such actions may be conducted secretly, as well as independently of the review of other departments and agencies with greater substantive experience,
and without the knowledge of other cabinet officials who have responsibilities for informing congress.58

For example, President Nixon's desire to ensure that he controlled U.S. foreign policy led him to support National Security Advisor Kissinger's efforts to direct a number of foreign policy issues, including normalizing bilateral relations with the People's Republic of China, conducting the war in Vietnam and eventually chairing the peace talks with North Vietnam in Paris. This led to a dominant role by the NSC staff in the development and implementation of policy in a number of areas while supporting the National Security Advisor. During the Nixon and Ford administrations (1973-1975), Henry Kissinger served concurrently as the National Security Advisor and Secretary of State. This arrangement most likely will never occur again, in part, because this arrangement defeats the objective of having the National Security Advisor act as an honest broker of policy among the various Executive Branch agencies involved in national security affairs.

Although the Secretary of State, by law, is responsible for the development and implementation of foreign policy, the President ultimately decides who among his national security team has what duties and responsibilities. Presidents who do not wish to be involved in the details and implementation of foreign policy delegate that authority to the Secretary of State. On the other hand, Presidents who wish to be intimately involved usually rely heavily upon the National Security Advisor to help formulate foreign policy and keep them updated on developments.

A President's willingness to delegate authority for managing specific national security issues to his National Security Advisor also occasionally has resulted in past NSC staffs assuming responsibility both for policy planning and execution. This is the situation that developed during the Reagan administration, resulting in the Iran-Contra affair referenced earlier in this report.

**Principals and Deputies Committees and the Policy Process**

The Principals Committee (PC) acts as the President's senior level policy review and coordination group. In effect, the PC is the same as the National Security Council without the President and Vice President (although Vice President Cheney regularly participated in PC meetings during the Bush administration). The PC's mission is to ensure that, as much as possible, policy decisions brought to the President reflect a consensus within the departments and agencies. If the process works as intended, the President does not have to spend time on uncoordinated policy recommendations and can focus on high level problems and those issues upon which the departments and agencies could not reach a consensus. In administrations where there are strong rivalries
among senior advisors (such as the Kissinger-Secretary of State Rogers enmity during the Nixon administration, or the competition between National Security Advisor Brzezinski and Secretary of State Vance during the Carter administration), policy coordination frequently breaks down. Even when strong disagreements (or rivalries) occur between senior policy advisors such as the Secretaries of State and Defense (e.g., Shultz and Weinberger during the Reagan administration, and Powell and Rumsfeld as reported during the first term of George W. Bush term), regularly scheduled PC meetings allow for such differences to be aired and identified, and consensus policy recommendations coordinated where agreement exists.

The frequency of Principals Committee meetings is driven primarily by the pace of events. It often meets once or twice each week to review policy on pressing matters, but may meet less or more frequently depending upon circumstances such as crisis situations or just prior to major summit meetings. Currently, the PC (or some variation if all the official PC members are not present) in the Obama administration meets several times each week based upon the number of issues requiring its attention. In addition (or sometimes in lieu of formal PC meetings), weekly informal meetings involving the Secretaries of State and Defense, and National Security Advisor are held over breakfast or lunch, or via secure telephone conference calls or secure video teleconferences (using the SVTS system). For the Obama administration, almost all PC meetings are conducted in person, with the SVTS system reserved for crises or other rapidly emerging situations. During the last year, meetings topics have included discussions of overall strategies for Iraq, Afghanistan, terrorism threats, political turmoil in the Middle East (the so-called “Arab Spring” phenomena), policy on U.S.-China strategic and economic relations, Japan’s tsunami and nuclear crisis, and relations with Pakistan, Haiti, North Korea, and Iran. Issues that are time sensitive and involve critical U.S. interests (such as the Japanese Tsunami, and the implications of the protests that overthrew the Mubarak regime in Egypt) are likely to be discussed at the PC level at first, but quickly fall under the responsibility of the Deputies Committee.

Likewise, the Deputies Committee (DC) meets when necessary, usually daily (and, at times, more than once in a single day), to review IPC recommendations, deliberate issues upon which the IPCs could not reach a consensus, and decide what matters should be forwarded to the PC. The Obama administration DC has favored face-to-face meetings for its senior policymaking groups (rather than teleconferences over SVTS) and tends to holds meetings in balance with the schedules and responsibilities of the deputies in their home departments. 59

Issues forwarded to the PC include a range of policy options, any consensus policy recommendations made at the DC and IPC level, and identification of policy issues upon which an interagency consensus could not be reached at the IPC and DC levels. In general, the DC seeks to review issue
papers and policy options and recommendations provided by IPC level groups and pass them up to the PC. Other than face-to-face or SVTS meetings to discuss policy issues, the PC and, especially the DC, also have an additional mechanism called the “paper PC” or “paper DC” process. In circumstances when a policy decision or action is called for and either there is insufficient time to bring PC or DC members together for a meeting, or the issue can be handled without the time required for a face-to-face (or SVTS) meeting, the National Security Advisor will circulate a written policy draft to PC or DC members to review, adjudicate, and return within a short period of time. The DC, which tends to review a wider range of policy issues (only the most important rise to the PC level), uses the “paper DC” process much more frequently than the PC. There are often four or five “paper DC” documents circulating at any one time.

During crisis periods, the PC, DC, and IPCs meet frequently. For example, during crises such as the 1991 Gulf War, 1999 Kosovo crisis, the aftermath of the terrorist attacks in September 2001, and the conduct of military operations in Afghanistan and Iraq, a typical day often included:

- **Departmental meetings with Secretaries or Deputy Secretaries in the early morning to review developments, responsibilities, taskings, and policy issues of concern to the mission of each department.**
- **In mid-morning, the DC meets, sometimes conducted via secure teleconferencing with senior staff and area-functional experts, to develop interagency positions on developments and new policy issues. This DC meeting might be followed immediately by a meeting of the DC senior members (without supporting staff) to discuss sensitive intelligence or policy issues.**
- **In late morning or early afternoon, the PC meets to discuss the results and unresolved issues of the DC, consider strategic policy directions, and determine what issues need to be brought to the attention of the President. PC members may then meet with the President (who usually receives updates on the crisis situation from the National Security Advisor throughout the day).**
- **In mid or late afternoon, the DC again meets to discuss the implementation of decisions reached by the PC and President, and to discuss the results of IPC meetings that have been held throughout the day (individual IPCs may meet more than once a day during crisis periods).**
- **Individual members of the DC are likely to have a late afternoon meeting with their principals to confer about developments of the day, and a subsequent meeting with their staffs to discuss the day’s decisions, developments, and next steps. Depending upon the circumstances of the day, the PC may have an additional evening meeting and subsequent consultation with the President.**
This kind of high operational tempo may persist for several weeks or months, depending upon the duration of the crisis and the need to involve the President and cabinet level officers on a daily basis. Not only do crisis situations alter the "normal" policy review and determination processes of an administration, but also, as noted above, the dynamics and processes will evolve in response to the President's preferences for managing the crisis. The national security policy apparatus is not a rigid system—it adapts to circumstances and operates according to what the President needs, wants, and supports.  

**Interagency Policy Committees and the Policy Process**

Interagency Policy Committees (IPCs) are responsible for a range of national security issues that cut across the responsibilities of Executive Branch departments and agencies. Issues may be regional, such as U.S. policy toward Iraq or NATO expansion, or functional, such as arms control agreements with Russia or terrorism in South Asia.

IPC work is different than that performed in the departments or agencies. Departmental or agency planning focuses on achieving agency objectives on a regional and operational level. Coordination is focused on departmental ways and means and is based upon internal agency doctrine and processes. Contentious issues are resolved internally at senior levels. IPC planning is focused more on advance planning at the political and strategic level. IPCs do the "heavy lifting" in analyzing policy issues and developing policy options and recommendations that provide policy-makers with flexibility and a range of options that are politically acceptable and minimize the risk of failure. Interagency groups also must develop policy options that advance U.S. interests through coordinated actions often involving many departments and agencies. An effective interagency process reduces the complexity of the policy decisions and focuses the planning on mission success factors. This means that policy planning must integrate desired policy aims and synchronize the efforts of the different departments and agencies. Planning to advance U.S. interests is likely to involve multi-agency and multilateral considerations.

Collaboration is central to an IPC's success, but teamwork and unity is vulnerable to political risks, bureaucratic equities, and personal relationships. Because U.S. interests and foreign policy have tended to remain fairly stable from administration to administration, an informal policy consensus often exists across agencies when dealing with routine matters. But, policy disagreements and turf battles are inevitable because of divergent political philosophies, different departmental objectives and priorities, disagreements about the dynamics or implications of developing situations, or because departments are seeking to evolve or formulate new roles and missions. Also, hard problems do not lend themselves to easy solutions, and frequently there are genuine differences between departments over the best ways, means, and objectives for
dealing with a national security problem. Moreover, because regional experts tend to dominate on overall policy approaches (even though they may lack expertise on many functional issues), different interpretations of events or credibility issues may arise within the IPC group. These issues must be openly addressed to enable the group to collaborate effectively, refine core policy issues, and achieve a consensus policy document. As one former NSC staff member observed, the easiest outcome to produce in the interagency process is to prevent policy from being made. The wide range of issues, the different policy perspectives of various departments, the nature of bureaucratic politics, contests over turf and responsibilities, disagreements over which department has the lead, and the clash of personalities and egos all place a premium on ensuring that the equities of all involved agencies are considered, and on building an informal policy consensus amongst the players.

The operational dynamics of individual IPCs, like most working group entities, vary according to the personalities (and, sometimes, personal agenda) of the individuals who are in charge of, or participate in them. In general, however, most IPCs undertake a five-part process when working on a policy issue:

- Define the problem. This includes assessing what U.S. national interests and strategic objectives are involved, reviewing intelligence reports, and seeking to determine some understanding of the dynamics of the situation (including what is known, what is assumed, and what is unknown) and the interests and motivations of the actors involved. Is there a consensus on the issues at stake for the U.S. and the implications of acting or not acting? This part of the process also includes identifying additional information and intelligence needs and levying requirements to the intelligence and diplomatic communities.

- Issue Terms of Reference. Develop broad principles to guide the way the interagency group should think about a problem and craft a strategy for addressing it. Clarify IPC processes and intra-group procedures for conducting meetings and accomplishing the task(s).

- Articulate policy objectives, assess options, and develop an overall strategy for U.S. policy. Deliberations may include preventive strategies, or strategies for responses to possible developments as policies are implemented. Mission areas for the departments and agencies should be clarified and component strategies (including identifying capabilities and resource needs) developed that, eventually, are integrated into a single strategic approach. “Straw man” proposals are useful for clarifying departmental perspectives. Strategies usually are required for consulting with friends and allies, and developing multilateral consensus on strategic objectives and operational activities. Other considerations include monitoring the implementation of complex, multi-dimensional activities.
(which may include the activities of several departments), and anticipating transition dynamics as policies begin to produce expected and unanticipated effects.

- Identify policy instruments and component strategies (including ways and means) to achieve the desired policy objectives. Operational planning must be clarified and coordinated among the agencies involved and integrated missions must be identified and coordinated where appropriate. A process must be developed that steers around interagency and bureaucratic roadblocks. The standard operating procedures in departments and agencies may have difficulty working with coordinated interagency plans and gaps may develop in implementation. IPCs must seek ways to talk with operational-level staff to determine potential problems and solicit suggestions for effective implementation.

- Draft an integrated policy options document. Ideally, this document should confirm the strategic approach, objectives, scope of effort and timelines, requirements and preparatory actions, chains of command, communication, and responsibilities (independent and shared) and accountability for the departments. It also should identify assets, resources, and logistical requirements. Mechanisms should be established for integration at all levels as policies are implemented. Key judgments about the situation, the important policy issues, and recommendations should be identified for the Deputies and Principals Committees. The Deputies and Principals need enough detail (but not too much) to be able to understand the dynamics of the situation, the major issues at stake, and implications for our national security. Depending upon the preferences of the incumbent administration, the IPC may be tasked to recommend a single policy option or multiple options, and provide majority and dissenting positions. Ideally, this process should include mechanisms for measuring the success of the policies, i.e., “metrics.” There also should be milestones set for completion of the various components of the policy to ensure implementers are clear that action is expected to be taken, and results reported back to senior policymakers.)

Although regional or functional IPCs deal with issues unique to their area of responsibility, there are a number of issues that most, if not all, IPCs find useful to consider. These include assessments of:

- Whether there is a compelling necessity for action. Are there threats to vital (or critical or important) U.S. interests? Is there an imperative for the U.S. to act? Are there viable alternatives to U.S. action?
- Desired U.S. objectives and the level of commitment to those objectives (by the departments and agencies, Congress, and U.S. public). Are the objectives clear and directly linked to U.S. interests?
• The level of U.S. resolve in its policy commitments as perceived by the countries the policies are targeted toward, other states in the region; allied, friendly, neutral and hostile states. The IPCs also should consider how the U.S. Congress and the U.S. public are likely to perceive the administration's resolve on proposed policies.

• The capabilities and willingness of allies, friends, and neutrals to support U.S. policy objectives and initiatives. Is there a consensus by key states or actors on the issue? What are their national interests? To what extent will they benefit or experience costs for supporting U.S. policy? What resources (political or otherwise) will they be willing to commit in support of the policy objectives; are they willing to act in a combined or coordinated manner?

• The likely reaction of regional states, allies, friends, neutrals, or hostile states that might oppose U.S. objectives. What are their calculations of costs and risks versus benefits to opposing the U.S.?

• The likely reaction of the United Nations or other international organizations to U.S. objectives. What are their calculations of costs versus benefits to supporting or opposing the U.S.?

• Costs and risks in implementing the policy versus costs and risks of inaction.

• Supporting or opposing legal authorities (e.g., international law, U.N. resolutions).

• The effects of stalled policy initiatives, and the administration's willingness to escalate (e.g., incentives, influence, coercion, etc.) to achieve policy objectives.

• Receptivity to considerations of alternative policies, and strategies for achieving the policy objectives in the face of stalled initiatives.

• The inherent limitations in trying to influence the course of events in achieving policy objectives.

• The effects of policy actions over time, including unintended consequences.

• Expected costs and benefits for those departments and agencies involved.

Some policy issues are even more complex and involve multidimensional assessments of allies and friends, neutrals, international organizations, and affected populations. For example, policy planning for peace operations, stabilization and reconstruction, or humanitarian missions would include consideration of issues related to:

• Diplomatic collaboration to solicit participants and build coalitions for delivering humanitarian assistance and deploying military forces (if required).

• The role of regional groups and organizations

• The role of the United Nations or other international organizations

• Cease-fire / disengagement / stabilization in the crisis area

• Prisoner exchange between warring parties

37

269
• Weapons control / demobilization
• De-mining
• Humanitarian relief
• Refugee / displaced person return
• Internal political cooperation
• Counter-insurgency and counter-terrorism
• Anti-official corruption / illicit criminal operations
• Strengthening local or regional institutions or organizations
• Management of factions / actors in the crisis area with political objectives incompatible with, or in direct opposition to U.S. objectives and who will seek to thwart U.S. actions
• Political transition / elections / democratization
• Rule of law / police / criminal justice
• Atrocities / abuses / war crimes prosecution
• Civil and social order
• National reconciliation
• Economic reform and restoration / private investment
• Public diplomacy
• Flash point management

Likewise, an IPC dealing with trade issues would involve considerations related to domestic and foreign economic and political issues, international laws and organizations, and different concerns for the departments and agencies involved.

Managing the process by which an IPC conducts business is complicated given the range and complexity of issues addressed. Lessons learned in the IPC process for promoting collaboration and high performance include maintaining a focus on a “high conceptual level.” This includes having participants support the following objectives:

Share an understanding of principles, goals, and priorities
• Bureaucratic interests must be represented, but remember that the final objective is good policy.
• Fully understand the policy context and preferences of their department principals, as well as those represented by others around the table.
• Expand individual frames of reference to gain an understanding of diplomatic, political, military, economic, humanitarian, development, and legal perspectives on the policy problem at hand.
• Seek a broad situation assessment, utilizing a wide range of intelligence, diplomatic, allies and friends, and NGO sources.
• Search for ambiguous assumptions and information gaps.
• Focus on a realistic time horizon.
• Clarify the tough value trade-offs in the policy decisions.
• Match commitments with political will.

**Support a prudent consensus approach**

• Agree on an effective process plan.
• Strengthen interagency team identity.
• Control internal politics among team members.
• Foster competitive—and constructive—debate.
• Prepare well thought out issue or policy positions backed up by data, examples, or persuasive points of argument.
• Forge a consensus approach for action. Internally, bring together opposing views and develop a consolidated position without diluting or ignoring important issues. Externally, build support with those sharing similar perspectives, and bring in supporting material from outside actors not directly involved in meetings but who can affect final acceptance of policy decisions (e.g., congressmen, staffers, trade interests, NGOs, etc.). This consideration should be weighed against the desires of higher level policy groups who prefer to have multiple analyses and options to contemplate in order to determine their own policy recommendations. Awareness of the preferences and operating styles of senior policy groups is crucial for working effectively at the IPC level.

• Keep your boss informed of developments, don't let him or her be blindsided in a higher-level policy forum.

**Maintain vigilance over intra-group management**

• Be well prepared on substantive issues, legal constraints, and the bureaucratic/policy preferences of your principal and the other agencies represented.
• Adjust and self-correct for changing conditions or ineffective group practices.
• Manage time, including competing commitments and responsibilities in order to advance the analytical and decision process and produce required policy products on time.
• Seek to be constructive and be willing to compromise and make trade offs.
• Participants in such meetings are not immune to considerations of their professional reputations and careers. Professionalism and the constructive handling of disagreements are important to successful operations.
• Keep pace—stay ahead of the crisis environment.
• Anticipate media/press issues and congressional concerns.

Meetings in response to crisis conditions are likely to experience additional complications. Crises are characterized by fast moving events, pressure to act quickly to minimize damage or prevent crisis escalation, partial and sometimes confusing or conflicting information or intelligence, and the
complexities of multi-tasking and coordinating the activities of a wide range of actors and interested parties. Moreover, in rapidly developing crisis situations similar to the post-September 11 period in the George W. Bush first term, IPCs may find that most policy decisions are handled at the PC and DC level. The IPC groups may find that they are dealing with regularly changing higher level policy directives, uncertainty about policy deliberations and decisions, and limited representative authority from their department to make decisions because the rapid pace of developments keeps most serious decision issues at the PC or DC level.

For the individual, the keys to being an effective member of a crisis management team are: (1) flexibility in thinking, (2) maintaining involvement, (3) maintaining alertness, (4) maintaining a strategic focus, (5) excellent writing skills, and (6) being unbiased.

- Flexibility in thinking. The preparation process for this annual report involves interviewing a range of experienced, senior USG officials who have served on or supported principals in high level policy groups. The one attribute most frequently mentioned by these senior officials over the years as needed for working effectively in interagency groups is flexibility in thinking. Participants must be able to understand the concerns and perspectives of other participants, quickly recognize new problems, and be creative in developing new approaches for dealing with problems. Reaching a consensus decision does not mean settling for the lowest common denominator, but instead balancing competing concerns to achieve the best policy recommendations for U.S. interests. Participants also must be able to understand the viewpoints of other participants and agencies, and capable of “re-framing” their perspectives on analyses and issues as events, actors, and interagency needs change. A firmly fixed view of the world and USG priorities becomes an obstacle to finding creative and effective solutions to complex, multi-dimensional problems.

- Maintaining involvement. Effective participation in working groups includes being an active team member, making insightful (but not redundant) contributions at meetings, knowing your department’s positions and equities, keeping senior officials in your department informed, staying abreast of the latest developments (e.g., reading the intelligence reports and embassy cables), doing a share of the drafting of papers, and being reliable (i.e., producing what you say you are going to do). This skill also includes being able to contribute to effective meeting dynamics in unstructured situations. This may include supporting processes that move the analytical and policy options and recommendation process along in an expeditious manner, and contributing to producing a high quality written document in a timely fashion.

- Maintaining alertness. Although self-evident at a superficial level, the day to day demands of working at the NSS or on interagency groups
can be grueling, often 12-14 hours a day, seven days a week. NSS Directors frequently work on 3-5 IPCs simultaneously, sometimes working multiple taskings from each group in addition to their normal staff responsibilities. Moreover, NSS Senior Directors also have responsibility for the 3-6 Directors who work under his or her supervision. Working in support of the president requires having physical and mental stamina. Crises that last weeks and months are even more physically and mentally demanding. They require perseverance and a willingness to spend long hours attending meetings and doing follow up work. During crisis situations, periods of threat, or rapidly developing events, IPC members may find themselves meeting several times a day over extended periods.

- Maintaining a strategic focus. Although individual working group members normally represent individual agencies, they must be able to concentrate on strategic interests and broad objectives, and not become mired in tactical or trivial issues that are the responsibilities of the policy implementing departments. They must keep in mind that they are writing recommendations for presidential action that must serve the interests of all agencies as well as the nation. Participants must be able to succinctly identify the critical central issues in frequently volatile, uncertain, complex and ambiguous situations.

- Excellent writing skills. NSC/NSS officials from the last 20 years identify accomplished writing, after substantive expertise, as one of the most essential skills required for working on the NSS. The typical policy issue paper written for the National Security Advisor or the President is only a couple of pages. IPC level issue papers on complex topics are only a few pages long. Working group members must be able to write short, well-organized documents which clearly and succinctly describe the policy issue being considered, why the issue is important enough to warrant presidential attention, and what options the President has for dealing with the situation. Participants must be able to think and write at the presidential level and present concise, clear analysis and arguments. A clearly written, well organized issue paper allows for more effective use of a senior policymaker’s time.

- Being unbiased means coming to working groups without personal agendas or pre-determined, inflexible positions. Effective participation on working groups requires the ability to be objective about different perspectives and aspects of policy issues and being able to develop balanced analyses and recommendations that take into account the many concerns and equities of the interagency. Written recommendations for the President must clearly present facts and data, what is known, unknown or assumed, without partiality. Participants also must be able to step back from the crisis periodically to see if interests, dynamics, or its strategic context have changed.
Effective IPCs must be able to periodically question assumptions established earlier in the crisis management cycle.

The HSC and the Policy Process

The primary role of the Homeland Security Council and the APHS/CT is to advise the President on homeland security and counterterrorism matters. Homeland security is a critical part of overall national security and increasingly has both national and international dimensions as the U.S. seeks to increase its security by promoting cooperation with international partners. As defined in the President’s National Strategy for Homeland Security (October 2007), “homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.” In the years since 9/11, the HSC has taken an “all hazards” approach to its mission of protecting the U.S. homeland from harm and homeland security programs focus on activities within the United States and its territories, supporting domestically-based systems and processes, or safeguard against external threats through visa screening, watch lists, the foreign government Container Screening Initiative, etc. The 2007 Homeland Security Strategy emphasizes leveraging a wide range of instruments of national power and influence “to prevent terrorism, protect the lives and livelihoods of the American people, and respond to and recover from incidents.” As such, Homeland Security policy involves a wide range of U.S. government agencies engaged in countering threats and protecting the country both at home and abroad.

In the post 9/11 security environment, U.S. national security issues encompass both foreign dangers and homeland security threats. Homeland security concerns include not only issues pertaining to attacks within the U.S. by foreign interests or factions, but also attacks perpetrated by domestic groups not affiliated with external organizations or nations. Homeland security also addresses public safety events that occur within U.S. borders, such as pandemic influenza, and responses to national disasters and emergencies such as Hurricanes Katrina and Rita that struck the U.S. Gulf coast in August and September of 2005, and the May 2010 Gulf of Mexico oil spill. Thus, while the NSC emphasizes national security trends and developments outside of the U.S. and combating terrorism overseas, at a minimum, national security and homeland security have large areas of overlapping responsibilities. This is particularly evident when examining the make-up of the National Security Council and the Homeland Security Council. Moreover, the steady evolution of homeland security threats involving both national and international dimensions was a major contributor to the merger of the NSC and HSC staffs into a single National Security Staff early in the Obama administration.
Regardless of its relationship to the NSC, the HSC has numerous homeland security priorities in policy development. These include supporting the President and his objective of ensuring the security of the United States, and ensuring that policies associated with homeland security are based upon strategic national security interests and not political pressures. A core function of the HSC is to recommend policies to the President that integrate various departmental and agency perspectives, and have been coordinated across the federal government state and local governments, as well as appropriate entities in the private sector. When circumstances involving global terrorism or other threats with domestic implications occur, the APHS/CT and the National Security Advisor have shared responsibilities and are expected to act in concert. Because homeland security involves a wide swath of domestic issues--some of which have significant international components (e.g., visa policy, port security, pandemic issues, etc.)--HSC coordination challenges can involve a wider range of domestically oriented Executive Branch agencies, the Congress, and state, local and private interests. Preventive planning considerations for homeland security that are likely to require state-level resource commitments; affect immigration, trade, or other economic issues; produce outcomes that are harder to visibly demonstrate (i.e., policies that produce greater security means that potential attacks are thwarted and become "non-events"); and affect a wide range of federal, state, and local (not to mention private sector) entities are highly likely to have local political as well as national security effects and implications.

In general, the HSC provides policy support to the President on homeland security matters. HSC serves as the conduit into and from the President (and other White House offices) on homeland security policy matters. The HSC is responsible for pulling together the perspectives of government agencies involved with homeland security matters that might be affected by proposed homeland security-related policy, and then coordinating those views through to a policy decision, and monitoring the implementation of the policy. The HSC deals mainly with domestic security policy issues, but also may play a major role in the consideration of issues and policy recommendations related to Canada, Mexico, other actors in the immediate CONUS geographic region, and, increasingly, states in other regions when potential homeland security issues may be involved. These bi-lateral policy issues may involve air transport security, visa screening and traveler watch lists, shipping container screening, maritime security, and border security. Although such issues are handled with the expanded NSS staff structure, they still fall under HSC policy areas rather than formal NSC policy responsibilities. HSC also is responsible for understanding the domestic implications of potential policy decisions in the homeland security area, and working with DHS which is responsible for coordinating with state and local officials both with regard to their responsibilities, on policies or DHS activities that affect state and local administrations and business.

Like the Principals Committee for the NSC, the PC for the HSC acts as the President's forum for senior level forum for policy review and coordination, and
seeks to ensure that, as much as possible, policy decisions brought to the President reflect a consensus between the relevant departments and agencies, but also clearly presents any unresolved disagreements (consensus is a goal—but not if the result is a policy reflecting the lowest common denominator of agreement). Typically the HSC PC meets regularly, but adjusts its frequency depending upon circumstances such as crisis situations or increased threat levels. The types of issues considered by the PC and DC of the HSC include prevent and disrupt terrorist attacks; protect critical infrastructure; respond to and recover from incidents (including natural disasters); cyber-security; bioterrorism; air, rail, road and maritime security; preparedness and protection against terrorism and natural disasters; information sharing; and coordination and communication with federal, state, and local authorities, as well as the private sector. The NSA, APHS/CT and the National Security Staff (as well as Principals and Deputies when appropriate) are responsible for ensuring interagency coordination with the Department of Homeland Security, other Cabinet Departments, and the Intelligence Community (including the National Counterterrorism Center (NCTC)). For example, the APHS/CT typically consults weekly with DHS officials and daily with the ODNI.

The HSC NSS IPCs analyze policy issues and develop policy options and recommendations that provide policy-makers with flexibility and a range of options that are politically acceptable and minimize the risk of failure. Interagency groups also must develop policy options that advance homeland security through coordinated actions often involving many departments and agencies, as well as state and local governments and the private sector. An effective interagency process reduces the complexity of the policy decisions and focuses the planning on mission success factors. This means that policy planning must integrate desired policy aims and synchronize the efforts of the different departments and agencies.

KEY DEPARTMENTS AND AGENCIES IN THE NATIONAL SECURITY POLICY PROCESS

Department of State

Under the U.S. Constitution, the Executive Branch and Congress have constitutional responsibilities for U.S. foreign policy. President George Washington's first cabinet included Secretary of State Thomas Jefferson. The Secretary of State is fourth in line of succession to the presidency.

Within the executive branch, the Department of State is the lead foreign affairs agency and the Secretary of State is the President’s principal foreign policy advisor. The Department also supports the foreign affairs activities of other U.S. Government entities, including the Department of Commerce and the Agency for International Development.
In addition, as the lead foreign affairs agency, the Department of State has the primary role in:

- Leading interagency coordination in developing and implementing foreign policy;
- Managing the foreign affairs budget and other foreign affairs resources;
- Leading and coordinating U.S. representation abroad, and conveying U.S. foreign policy to foreign governments and international organizations through U.S. embassies and consulates in foreign countries and diplomatic missions to international organizations;
- Conducting negotiations and concluding agreements and treaties on issues ranging from trade to nuclear weapons; and
- Coordinating and supporting international activities of other U.S. agencies and officials.

The Department of State, like many other cabinet departments, is a centralized organization, with the Secretary of State at the helm. Beneath the Secretary in the senior hierarchy are other senior officials, including a Deputy Secretary of State for policy, a Deputy Secretary of State for Management and Resources, and the Counselor of the Department. Beneath the Deputy Secretaries are a series of Under Secretaries responsible for policy and management areas. Assistant Secretaries for regional and functional bureaus then follow in terms of authority and responsibilities. (See Appendix D for a State Department organizational chart)

Although the Department of State is the lead government foreign affairs agency, it does not dictate foreign policy for the U.S. government. Because so many executive branch departments have international programs, there is an inherent difference in perspective at interagency meetings. Secretary Colin Powell, in his testimony before Congress (April 23, 2003), addressed the phenomenon in this way: “With respect to what’s going on within the administration, it’s not the first time I have seen discussions within the administration between one department and another. I have seen four straight administrations at a senior level; and thus it has been, and thus it has always been, and thus it should be. There should be tension within the national security team, and from that tension, arguments are surfaced for the President. And the one who decides, the one who makes the foreign policy decisions for the United States of America, is not the Secretary of State, or the Secretary of Defense or the National Security Advisor. It’s the President.”

In conducting international affairs, the Secretary attends cabinet meetings, NSC meetings, and PCs chaired by the National Security Advisor. When the Secretary is traveling abroad, a deputy may be designated to attend as State’s senior representative. For example, Secretary of State Hillary Clinton designated former Deputy Secretary Steinberg to attend PCs in her absence. Similarly,
Deputy Secretary Steinberg asked Under Secretaries or Assistant Secretaries to attend DCs. Under Secretary for Political Affairs William Burns (who replaced Steinberg as Deputy Secretary) is a prime example of an under secretary who has attended PCs and DCs, in part because of the expertise he brings to bear. Regarding IPCs, assistant secretaries or their deputies usually attend. Delegating others to attend interagency meetings has been a fairly common practice in all administrations.

Frequently, special senior interagency committees are established. During the Clinton administration, an interagency "Coordinating Sub Group" on terrorism, whose members included State's Ambassador for Counter-Terrorism Affairs and similarly ranked officials from DOD, FBI and CIA, met under the chairmanship of a senior NSC official. This practice persists in the current Obama administration. For example, there is an "Executive Steering Group", chaired by a senior NSC advisor, which deals with a wide variety of issues (including Iraq) and a Counter-Terrorism Security Group that reports directly to the Deputies Committee.

After the August 1998 bombings at the U.S. embassies in Kenya and Tanzania, Secretary of State Albright appointed Accountability Review Boards (ARBs) for both events. These boards were chaired by the late Admiral William Crowe, a former Chairman of the Joint Chiefs of Staff and later U.S. Ambassador to Great Britain. This was done in accordance with U.S. laws that mandate convening such boards anytime there is a security-related incident causing serious injury, loss of life, or significant damage of property at or related to a U.S. mission abroad. In brief, ARBs investigate and to make recommendations. Retired and active duty representatives from State, the FBI, CIA, and the private sector served on the two boards.

Among the recommendations from the ARBs chaired by Crowe was an appropriation of $1.4 billion a year for at least ten years for embassy construction and repair. Madeleine Albright writes in her autobiography: "By the time I left office, we had gained agreement for appropriations close to the level recommended by Admiral Crowe, an agreement that was critical because we had learned that the dangers to our personnel were no longer localized but global. There was no such thing as a low-risk post. If we had soft spots, we could expect our enemies to exploit them." The program to secure U.S. facilities overseas continues with $1.4B per year as the basis for the Capital Security Cost Sharing program. Each agency having an overseas presence is expected to contribute to the $1.4B total.

Below this level, there are numerous other interagency groups. They may meet recurrently or just once. After Saddam Hussein's invasion of Kuwait and Operation Desert Storm, there were a series of interagency sessions on a wide range of U.S. policy issues in the Gulf. Similarly, during the Clinton administration, the State Department called a one-time interagency meeting on
Lebanon when the issue of the passport restriction on American citizens was under review. Officers at the GS-15 or equivalent rank were asked to attend from a wide array of agencies—DOD, FAA, CIA and the like. Likewise, a variety of interagency meetings were held before, during and after Operation Iraqi Freedom. The purpose of such meetings may not be to decide the issue, but to exchange views and lay groundwork for issues expected to be considered by IPCs, DCs, and PCs. Staff work for such meetings may be narrowly focused, and handled even by a single office in a bureau.

One State Department office created explicitly for the purpose of promoting interagency collaboration on policy development and execution is the Office of the Coordinator for Reconstruction and Stabilization (S/CRS). Established on August 5, 2004, the mission of S/CRS is “to lead, coordinate and institutionalize U.S. Government civilian capacity to prevent or prepare for post-conflict situations, and to help stabilize and reconstruct societies in transition from conflict or civil strife, so they can reach a sustainable path toward peace, democracy and a market economy.” The State Department’s authority for this mission is derived from National Security Presidential Directive-44 (NSPD-44) concerning the “Management of Interagency Efforts Concerning Reconstruction and Stabilization” which directs the Secretary of State to “coordinate and lead integrated United States Government efforts, involving all U.S. Departments and Agencies with relevant capabilities, to prepare, plan for, and conduct stabilization and reconstruction activities.” Working under the authority of NSPD-44, S/CRS has established a number of sub-IPC working groups to plan, prepare, and conduct stabilization and reconstruction missions. The office works with the U.S. Agency for International Development (USAID), the Office of the Secretary of Defense, the Joint Staff, Justice, Treasury, the Department of Labor, Office of Management and Budget and other government agencies to devise interagency organizational structures, identify resource requirements and prepare interagency mobilization plans, coordinate political-military planning for stabilization and reconstruction operations, conduct decision support exercises and prepare implementation strategies.

The staff work done for the Secretary of State and his or her principals for interagency meetings is a complex and highly organized undertaking. The Office of the Executive Secretary (S/ES) is key. S/ES is located on State’s “seventh floor” and is comprised of some 175 plus employees. It is responsible for coordinating State Department’s internal operations, liaising between the bureaus and principals, running the State Department’s 24/7 operations center, organizing and staffing the Secretary’s foreign travel, and liaising between the NSC and other executive branch departments. More specifically, S/ES is responsible for tasking papers within the State Department for the Secretary’s international trips and for interagency meetings involving Department principals. S/ES sets the due dates for these papers in line with the time of the meetings.
An Executive Secretary and three Deputy Executive Secretaries lead S/ES. The Executive Secretary traditionally is a senior career Foreign Service officer.

The relationship between State's Executive Secretary and Executive Secretaries in the National Security Council and the Department of Defense is very important. It is often through their communications, both verbally and in writing that notification of high-level meetings is made. State Executive Secretaries also may receive debriefs from their counterparts on decisions from more informal meetings or discussions among the Secretary of State, Secretary of Defense, and National Security Advisor.

One aspect of the State Department which sets it apart vis-a-vis the interagency process is its own special composition. In his memoirs, James Baker, former Secretary of State under Bush 41, wrote that, "Without a doubt, the State Department has the most unique bureaucratic culture I've ever encountered. In most of the federal government, the work is guided by a small number of political appointees who work together with civil service—the career bureaucracy that is designated to be above politics and provide institutional memory and substantive expertise. But at State there is also the Foreign Service, the elite corps of foreign affairs officers who staff the Department's country and functional desks in Washington and our embassies abroad." 69

At interagency meetings, the State Department representatives, whether in support of a principal or on their own, bring to the table a wealth of on the ground, in-depth experiences in dealing with foreign governments and cultures from around the globe, which helps frame their recommendations and conclusions. In addition, by virtue of State's position as the lead government agency in foreign affairs, the State Department has an unusual breadth of information to tap—from all agencies. In his memoirs, Secretary Shultz wrote that, "As Secretary, I could see that I had at hand an extraordinary information machine: it could produce a flow of reports on what was happening in real time, background on what had been done before and how that had worked, analyses of alternative courses of action, and ideas on what might be done. The Department is a great engine of diplomacy for the Secretary to use in carrying out the president's foreign policy." 70

Department of Defense

To understand and have an appreciation of the Department of Defense's (DOD's) role in the interagency process, it is instructive to look briefly at DOD's history and how it evolved into the organization it is today.

First, one should remember that the department did not exist, nor did the Joint Chiefs of Staff (JCS), until the late 1940s. Up until and through the Second World War, there were two military departments—War and Navy. Both the Secretary of War and Secretary of the Navy reported directly to the President.
Conflicting judgments often arose between the Army and Navy over critical issues, including allocation of resources, strategic priorities, and command arrangements. Disagreements sometimes affected how military operations were conducted. To coordinate efforts during WW II, some 75 inter-service agencies and inter-departmental committees were formed. These ad hoc arrangements worked, but only because of the nation’s vast resources were we able to compensate for mistakes, inefficiencies, and internal divisions.

The National Security Act of 1947 created a National Military Establishment (NME) headed by a Secretary of Defense. The three secretaries of the military departments (including the Secretary of the newly formed Air Force) retained their powers, subject only to the authority of the Secretary of Defense to exercise “general direction, authority, and control.” The newly formed National Security Council (NSC), chaired by the President, included the Secretaries of State, Defense, Army, Navy, and Air Force, and the Chairman of the National Security Resources Board. During this nascent phase of the NSC, the military’s perspectives were well represented by occupying four of the seven NSC seats.

The NME was replaced by the DOD under provisions of the 1949 Amendment to the National Security Act. The 1949 Amendment also increased the powers of the Secretary of Defense, diminished those of the military departments, and provided for a Chairman with no direct military command function to preside over the JCS (and the Service Chiefs as a corporate body). Moreover, with this amendment, the secretaries of the military departments lost their membership on the NSC.

There were two legislative acts during the Eisenhower administration (1953 and 1958) that consolidated more authority in the hands of the Secretary of Defense. Given President Eisenhower’s military background, it should be no surprise that he was a firm believer in centralized control and a clearly defined chain of command. A fairly strong Secretary of Defense, together with a weakly structured JCS that functioned as a committee, prevailed through the 1960s (mainly the McNamara years) and the 1970s. It was not until the Goldwater-Nichols Act of 1986 that the military gained a greater voice in interagency affairs. The Act provided, among other things, for a stronger Chairman of the Joint Chiefs of Staff (CJCS) who would be the principal advisor to the President, the NSC, and Secretary of Defense (as compared to a Chairman who previously represented the views of the four Chiefs of the Services). Goldwater-Nichols also significantly increased the powers of the combatant commanders and clarified the chain of command from the President to the Secretary of Defense to the unified commanders. This ascension of the commanders, in effect, further weakened the influence of the individual service secretaries and chiefs.

Today, the DOD is a centralized organization where the Secretary of Defense exercises authority, direction and control over the DOD, and serves as a
member of the President's Cabinet and the NSC. The Secretary of Defense, together with the Commander-in-Chief, epitomizes the principle of "civilian control of the military." Ultimate authority within the Department of Defense rests with the Secretary. The three Service Secretaries report directly to him, as do the senior civilian officials in the Office of the Secretary of Defense. The Chairman of the Joint Chiefs of Staff (CJCS) is the senior ranking member of the U.S. armed forces and the principal military advisor to the President and the Secretary of Defense, but by law does not exercise military command. While the unified combatant commanders, by statute, report to the Secretary of Defense, by practice they clear (or at least discuss) all positions with the CJCS prior to communicating with the Secretary. The JCS refers to the Joint Chiefs of Staff of the Service Chiefs, while the Joint Staff refers to the staff that works directly for the Chairman, CJCS, not for the JCS (See Appendix F for a Defense Department organizational chart).

The Secretary of Defense and CJCS are the primary Defense players in the national level interagency arena. They represent the Department at NSC meetings chaired by the President, and at Principal Committee meetings chaired by the National Security Advisor. Their deputies, the Deputy Secretary of Defense and Vice Chairman of the Joint Chiefs of Staff, attend the Deputies Committee meetings (throughout the first Bush and the Clinton administrations, however, the Secretary of Defense was represented at the DC meetings by the Under Secretary of Defense for Policy).

At the staff level, virtually all the work in DOD for interagency deliberations is done in the Policy organization for the Office of the Secretary of Defense (OSD) and in the J-5 directorate (Strategy, Plans and Policy) for the Joint Staff. Attendees at the Policy Coordination Committee meetings and lower-level interagency groups are Assistant Secretaries, Deputy Assistant Secretaries, and GS-15s from Policy and one- or two-star flag officers and action officers (O-5s and O-6s) from J-5. With regard to homeland defense and civil support issues, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs is the single point of contact for the many directorates and agencies within the DOD.

Historically, it was uncommon for representatives from the unified commands or the individual services to attend the most senior level interagency meetings. The possible exception might be if a combatant commander is specifically invited by the President (or National Security Advisor) to attend a meeting. The Joint Staff typically represents the combatant commanders in interagency meetings. The Joint Staff is quite protective of the fact that they work to fulfill the statutory responsibilities of the CJCS as the principal military advisor to the President, the Secretary of Defense, the NSC, and the HSC. (The Joint Staff worked for the JCS as a body prior to Goldwater-Nichols. Now they work directly for the Chairman. The lack of command function for the CJCS and Joint Staff was directed by Congress to prevent the development of a
centralized "general staff" which might develop too much power. Specifically, they wished to avoid the possibility of replicating the control of strategy held by the German General Staff during the two World Wars.)

The advent of U.S. military interventions in Iraq and Afghanistan, combined with enhanced teleconferencing upgrades to the White House Situation room, have led to increased participation by theater commanders in SVTS sessions with the President. For example, during the U.S. "surge" of military forces into the Baghdad region during 2007, General David Petraeus, the Commander of Multi-National Force-Iraq, participated in SVTS sessions with President Bush to discuss developments in the country. Likewise, General Petraeus, as the Commander, International Security Assistance Force (ISAF) and Commander, U.S. Forces Afghanistan, regularly participates in SVTS conferences with President Obama and his national security team. Moreover, widespread VTC capabilities have facilitated increased participation by military commands in lower level interagency VTC conferences. For example, since 2009 the Pentagon has hosted a weekly Pakistan-Afghanistan Federation Forum VTC that includes various U.S. military commands in the U.S. and around the world, the State Department in Washington, D.C. and overseas embassies, White House NSS staff members, the U.S. Agency for International Development, and other executive branch agencies. VTC forums such as the PAK-AF forum allow the military and civilian interagency components concerned with specific national security issues to share information and plan strategy on a regular basis.

Some Presidents have preferred to hear a coordinated DOD position while others wished to hear counter-arguments and multiple options. Especially since Goldwater-Nichols, the military’s views should be submitted separately from OSD’s. However, crisis conditions may affect the President’s willingness to pursue extensive debates on competing options. For example, after the September 11, 2001 terrorist attacks, the Secretary of Defense and Deputy Secretary of Defense expressed opinions at a strategy session of senior Presidential advisors. At the conclusion of the meeting, the President’s Chief of Staff pulled the two participants aside and admonished, “The President will expect one person to speak for the Department of Defense.” Some DOD officials believe strongly that if the OSD civilians and the military have a coordinated position and speak as one voice, the Department’s views carry more weight and DOD officials can be more effective in the interagency process.

Another example of differing voices occurred during the initial deliberations in August 1990 after Iraq invaded Kuwait. After a meeting with the President, then Secretary of Defense Cheney chastised General Powell, then the CJCS, for offering an opinion that the Secretary perceived as political advice. "Colin," he said, "you’re the Chairman of the Joint Chiefs. You’re not Secretary of State. You’re not the National Security Advisor anymore. And you’re not Secretary of Defense. So stick to military matters."
This is not to say, however, that military officers should not speak at interagency meetings. They should speak. They are obliged to give their best military advice on the issue at hand. Often, military officers are criticized for not speaking out more forcefully. Their reluctance to speak might be because they do not want to be viewed (especially at the lower officer levels) as presenting the views of the CJCS. Another reason for their reluctance may be more personality driven, i.e., a certain amount of intimidation by the senior civilians around the table. Nevertheless, some senior flag officers believe strongly that military officers also should comment on non-military matters. They argue that military officers bring a strategic perspective to interagency groups that can help clarify (or question) assumptions, identify conflicting interests, or raise questions about unintended second or third order effects of proposed policies. One former DC participant with extensive government experience recommended that military officers educate themselves more broadly on national security issues (including resource and economic issues, homeland defense and security, intra-state conflict, refugees and migration, etc.) to be able to better understand how military roles and missions may affect, or are affected by, such traditionally non-military policy issues that increasingly involve or constrain military planning.

Even so, it is important that the proper military advice be given (with officers clearly delineating whether they are representing the "position of the Chairman" or based upon their own expertise). Most of the civilians at interagency meetings have little or no experience with military operations. They generally do not have an appreciation for what happens "behind the scenes" of any successful military operation. Without getting into the weeds, military officers need to explain what could be accomplished with the use of military forces, as well as the limitations and potential consequences in using such forces. At the same time, the military should expect at the conclusion of these deliberations to have a clear set of objectives and parameters within which to operate. It is critical that DOD, and especially the uniformed military, be fully engaged in debates taking place in the White House by civilians when use of the military instrument of national policy is being considered.

Traditionally, the DOD performs a secondary (or support) role to State’s lead in foreign policy, but plays an active role at interagency meetings in determining the parameters, or tools, of our foreign policy. From DOD’s perspective, three primary concerns are: possible uses of military forces; expenditure of Defense resources; and preventing a situation from deteriorating to the point that it requires military intervention.

In some circumstances, DOD plays a more than equal role in foreign policy discussions because of coalition military considerations and political-military and security issues (e.g., civil-military, nation-building and/or stability operations in Afghanistan and Iraq). Historically, though, DOD frequently has resisted the involvement of U.S. troops because situations were assessed to not
constitute a proper military mission or there are other alternatives available (i.e., other countries' military forces, UN, NGOs). The Department's position in such meetings often is to withhold use of U.S. forces unless they, and only they, possess the capability to perform a function that protects or promotes U.S. security interests.

The second frequent DOD concern is the expenditure of resources. Policymakers rarely consider the cost of operations directed by the NSC. This usually is due to the urgency of taking action or a tendency to ignore (or avoid) the fact that ultimately someone has to pay the bill. There also is a common belief that "DOD possesses all the resources." While it is true that Defense's budget is larger than the Department of State's, laws and regulations govern precisely how and for what purposes DOD's money may be spent. So, just as use of military forces is not necessarily the best, or only, solution, careful attention needs to be paid to the cost of such actions taken through the interagency process, and to who will pay those costs.

The third concern is preventing a situation from deteriorating to the point that it requires military intervention. DOD plays an active role in interagency meetings shaping the strategic situation in many regions of the world. DOD strives to ensure that USG policy and resources are adequately coordinated to shape the environment and obtain results favorable to U.S. interests. Working closely with the Department of State, USAID and other agencies, DOD's involvement in regional programs can be the catalyst for policy changes that could avert future military intervention. An example of this was DOD's active role in changing USG policy regarding Colombia. Until 2002, U.S. policy for Colombia was primarily based upon helping Colombia reduce its drug production. After 9/11, DOD lobbied hard for a change in the policy and was successful in getting a PC to authorize the development of a new NSPD for Colombia. DOD led the effort to produce NSPD 18 in November 2002--in effect changing the Colombia policy from counter-drug to counter-narcoterrorism. This policy's immediate impact was the strengthening of the Colombian government and avoiding potential instability that could have triggered a request for U.S. military intervention.

Ultimately the decision to use military forces may be based upon political interests and not DOD's judgments about the "best" use of combatant forces. For example, in the days leading up to the decision to deploy U.S. forces into Somalia in 1992 to assist humanitarian operations responding to widespread famine, the combatant commander of the US Central Command (USCENTCOM) argued about the deleterious impact on military readiness for dealing with potential threats to higher level U.S. interests in the Persian Gulf and broader Middle East region. Nevertheless, the political decision that the acute humanitarian and U.S. international leadership interests at the time required U.S. intervention. These political interests overrode DOD's concerns about the impact on traditional mission capabilities.
The terrorist attacks of September 11, 2001, as well as the 2004 Indian Ocean Tsunami disaster response operations, and the 2005 Hurricanes Katrina and Rita disaster response operations broadened the scope of DOD’s contacts, roles and missions in the interagency arena. In response to the terrorist attacks and the need for greater coordination and integrated operations with mission partners, DOD approved the concept of Joint Interagency Coordination Groups (JIACG) to improve interagency cooperation and improve operational effectiveness for all Geographic Combatant Commands, USJFCOM, USTRANSCOM, USSOCOM, and USSTRATCOM. JIACGs are tailored to meet the requirements and challenges of each Combatant Commander’s AOR, and may include representatives from a wide range of USG agencies, the intelligence community, as well as private voluntary or non-governmental organizations (PVOs or NGOs) such as the American Red Cross.

The JIACG concept seeks to establish operational connections between civilian and military departments and agencies that will improve planning and coordination within the government. The JIACG is a multi-functional, advisory element that represents the civilian departments and agencies and facilitates information sharing across the interagency community. It provides regular, timely, and collaborative day-to-day working relationships between civilian and military operational planners. JIACGs support Joint Planning Groups, Joint Operations Groups, Interagency Coordination Groups, and Joint Support Cells.

JIACGs complement the interagency coordination that takes place at the strategic level through the National Security Council System (NSCS). Members participate in deliberate, crisis, and transition planning, and provide links back to their parent civilian agencies to help synchronize joint task force (JTF) operations with the efforts of civilian USG agencies and departments.

JIACG functions include:
- Participate in combatant command staff crisis planning and assessment.
- Advise the combatant command staff on civilian agency campaign planning.
- Work civilian-military campaign planning issues.
- Provide civilian agency perspectives during military operational planning activities and exercises.
- Present unique civilian agency approaches, capabilities, requirements and limitations to the military campaign planners.
- Provide vital links to Washington civilian agency campaign planners.
- Arrange interfaces for a number of useful agency crisis planning activities.
- Conduct outreach to key civilian domestic, international, intergovernmental, regional, and Private Sector/Non-Governmental (PS/NGO) contacts.

In day-to-day planning at the combatant commander headquarters, the JIACG group supports planners by advising on civilian agency operations and plans, and providing perspective on civilian agency approaches, capabilities and
limitations to develop a coordinated use of national power. For example, USEUCOM identifies the mission of its USEUCOM Plans and Operations Center Joint Interagency Coordination Group (EPOC-JIACG) to be: "Synchronizes, coordinates, and integrates USEUCOM, DOD and non-DOD U.S. governmental agency joint, joint interagency, combined, and joint/combined interagency counterterrorist (CT) operations within the USEUCOM Area of Operations and, in concert with other unified combatant commands, within the USEUCOM Area of Interest. Resources permitting, EPOC-JIACG (CT) expands beyond CT to support the full spectrum of conflict."  

When a joint task force forms and deploys, the JIACG extends this support to the commander's staff through the JFHQ political-military planning staff. This becomes the mechanism to plan the best mix of capabilities to achieve the desired effects that include the full range of diplomatic, information, and economic interagency activities.

In the aftermath of September 11, DOD also established the United States Northern Command (See Appendix G for a USNORTHCOM organizational chart). The command's mission is to conduct homeland defense, civil support and security cooperation to defend and secure the United States and its interests. The area of responsibility (AOR) includes the U.S. (minus Hawaii which is in US Pacific Command's AOR), Canada, Mexico, Puerto Rico, the Virgin Islands, Bahamas, Turks and Caicos Islands, and associated Maritime areas. USNORTHCOM has both a homeland defense mission and a civil support mission including defense support of civilian authorities (DSCA) operations as directed by the President or Secretary of Defense.

The Commander of USNORTHCOM is dual-hatted as the NORAD Commander. NORAD conducts aerospace warning, aerospace control, and maritime warning in defense of North America. NORAD has unique security relationships with various interagency partners in the U.S. and Canada. Close working relationships with The Royal Canadian Mounted Police, DHS's Customs and Border Protection, and Department of Justice's Federal Bureau of Investigation link both countries together in the day-to-day air defense of North America. This dual command arrangement is unique in the sense that NORAD and USNORTHCOM mission areas have direct implications for both HSC and NSC policy matters. The USNORTHCOM organization reflects the complexity of its AOR. To facilitate coordination with federal, state and local agencies, the Command has a robust Interagency Coordination (IC) directorate headed by a Senior Executive Service (SES) official. In concert with the Assistant Secretary of Defense for Homeland Defense & America's Security Affairs, interagency activities range from incident response, to operational planning, to Theater Security Cooperation and Building Partnership Capacity programs and efforts, to joint exercises between the Department of Homeland Security and USNORTHCOM. These joint exercises include multiple hazard chemical, biological, radiological, and nuclear (CBRN) incidents; threats to infrastructure,
aviation, or shipping facilities; airport, port, and border security; and support to civil authorities.

USNORTHCOM works closely with the Department of Homeland Security and other Federal agencies on issues pertaining to Homeland Defense and Homeland Security such as coordinating and de-conflicting responsibilities for maritime awareness and interdiction, and counter-drug and counter-narcoterrorism operations. When directed by the President or Secretary of Defense, USNORTHCOM provides defense support of civil authorities (i.e., DSCA, including responding to requests for assistance (RFAs) when local, state, or Federal agencies need DOD capabilities such as aviation support, specialized medical support, etc.) and also coordinates with the National Guard to integrate their capabilities when they are in State or Federal status. The homeland defense/civil support requirements for USNORTHCOM necessitate that it often is involved in very non-traditional operations for a geographic combatant command.

Recent examples of NORAD and USNORTHCOM activities include support for recovery operations of the Space Shuttle Columbia disaster, military support for the United Nations General Assembly, G-8/G-20 Summits, Democratic and Republican National Conventions, POTUS protection, and Presidential inaugurations and funerals. Moreover, NORAD continues to provide Operation NOBLE EAGLE combat air patrols ensuring air defense coverage for North America, including the National Capital Region (NCR) and during National Special Security Events (NSSE). In support of NSSEs, POTUS protection, and NCR security, NORAD and USNORTHCOM work daily with the United States Secret Service, Transportation Security Administration, Federal Aviation Administration, Transport Canada, and numerous other interagency partners both in the U.S. and Canada. In the NCR, the multi-domain NCR Coordination Center (NCRCC) has representatives from the NORAD Eastern Air Defense Sector in the same facility with all federal agencies involved with aviation security in the NCR.

Some of USNORTHCOM’s unique challenges include:
- Planning for active duty, reserve, and National Guard requirement contingencies for homeland defense or civil support.
- Planning for prevention, response, and consequence management for the possibility of multiple, simultaneous geographically dispersed terrorist incidents in CONUS.
- Managing planning requirements since USNORTHCOM has a limited number of assigned forces for civil support. In the event of incidents that might require the use of military forces in CONUS, USNORTHCOM is responsible for specifying to DOD what capabilities are needed. The inherent time delay in this process and the training capabilities or shortfalls of available forces are important issues, especially when put in the context of responding in a timely and effective manner to 9/11 and/or Hurricane Katrina level (or greater) homeland events.
• Advocating for homeland defense planning to be fully integrated into planning for more traditional security issues such as WMD, force projection, regional security concerns, etc.
• Planning for integrating and synchronizing the activities of DOD, DHS, DOJ, state and local entities, and NGOs to ensure mutual understanding and unity of effort. USNORTHCOM coordinates with the interagency community so that mechanisms for CONUS incidents will be driven by the type of problem encountered rather than by pre-set bureaucratic structures.
• Providing early situational awareness, conduct effective operations when required, and facilitate planning for future operations.
• Promoting information sharing between USNORTHCOM and federal, state, local, and PS/NGO partners.
• Enhancing interoperable communications during catastrophic disasters to be able to provide support where needed, when needed. Viable and interoperable communication nodes are necessary to expedite USNORTHCOM's assistance and to target support where the critical need exists.
• Establishing a Common Operating Picture. Catastrophic disasters mandate a requirement for quick assessment of the situation and support needs from affected locations. The Federal Government and USNORTHCOM require real time information about the magnitude and effects of natural and manmade disasters to properly, and promptly, tailor effective DOD support to Homeland Defense and Civil Support partners.

It is important that the proper military advice be given (with officers clearly delineating who they represent). Many of the civilians at interagency meetings have little or no experience with military operations. They generally do not have an appreciation for what happens “behind the scenes” of any successful military operation. Military officers need to explain what could be accomplished with the use of military forces, as well as the limitations and potential consequences in using such forces. At the same time, the military should expect at the conclusion of these deliberations to have a clear set objectives and parameters within which to operate. However, military officers also must recognize that changing political developments that often accompany military operations may necessitate changes in previously established objectives and parameters. What often is characterized as “mission creep” in the media often is the result of a re-evaluation of interests and policies because of changing political conditions on the ground or at the strategic level. Nevertheless, it is critical that DOD, and especially the uniformed military, be fully engaged in debates taking place in the White House when decisions about the military instrument of national policy are being considered.
The Intelligence Community

The primary role of the intelligence community in the process of national security decision-making is to provide information and analysis of that information to help policy-makers (including war-fighters and those in the law enforcement communities) understand the elements and dynamics of the various situations they must address. Information provided by the Director of National Intelligence, Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, Federal Bureau of Investigation, and other intelligence community components contributes to the overall assessment about what is happening on the ground, what is the nature of the concern in a particular geographic area, who are the actors, what are their dispositions, and what are their likely capabilities and intentions. The latter is the most difficult analysis for the intelligence community to produce and may sometimes result in differing opinions and predictions, based upon the inherently subjective nature such analysis. (See Appendix H for an Intelligence Community organizational chart)

The Office of the Director of National Intelligence (ODNI) was established in December 2004 by the Intelligence Reform and Terrorism Prevention Act of 2004, further amending the National Security Act of 1947. The Director of National Intelligence (DNI), who is appointed by the President and confirmed by the U.S. Senate, is the principal adviser to the President and National Security Council for intelligence matters related to national security, and serves as the head of the U.S. intelligence community. The DNI establishes objectives, priorities, and guidance for the intelligence community and manages and directs tasking of collection, analysis, production, and dissemination of national intelligence. The DNI approves requirements for collection and analysis, including requirements responding to the needs of policymakers and other intelligence consumers. The DNI also has responsibility for developing and monitoring the execution of the National Intelligence Program (NIP) budget and provides budget guidance to intelligence elements of departments and agencies that are outside of the NIP. The DNI has the authority to establish national intelligence centers as necessary and is responsible for the National Intelligence Council (NIC) which produces National Intelligence Estimates. The DNI also is responsible for ensuring accurate all-source intelligence, competitive analysis and that alternative views are brought to the attention of policymakers, and included in the President’s Daily Brief (PDB).

Since the establishment of the ODNI in 2004 and the appointment of its first director in April 2005, the DNI has undertaken the role of primary intelligence advisor to the President and the NSC, replacing the Director of Central Intelligence (DCI). The DNI serves on the Principals Committee (PC), and likewise, the DNI Principal Deputy Director serves on the Deputies Committee (DC). However, the Director of the Central Intelligence Agency (DCIA) and DDCIA attend NSC, PC and DC meetings (respectively) when appropriate per
CIA authorities and equities. The DNI also has the authority to issue binding policy directives for the intelligence community.

Established to oversee and direct the implementation of the National Intelligence Program, the ODNI serves as an interface between the Intelligence Community and policymakers to set the national priorities for intelligence collection and analysis. Significant intelligence taskers are routed through the ODNI to ensure proper coordination, although finished intelligence products often move directly from each agency to NSC members and other policymakers. Many other responsibilities and functions of intelligence community components (such as the CIA, NSA, NGA, etc.) have not changed with the establishment of the ODNI. Of note, though, the ODNI is now responsible for the President's Daily Brief, with input from across the Community. Whenever covert action activities are being considered, the DCIA is involved because the CIA retains its responsibility as the executive agency responsible for covert operations (i.e., secretly executed actions which implement policy directives of the President).

Including representatives from the various elements in the intelligence community in IPCs or other national security policy planning groups is often critical because reviewing existing intelligence information and determining requirements for additional intelligence collection and analysis should be one of the first steps in considering national security issues. The National Intelligence Managers at ODNI also serve this coordinating function for many issues or geographic areas of interest. Analysis from the intelligence community will help decision-makers better understand conditions (political, social, economic, military, transportation, communications, public health, environmental, etc.) in other countries, the capabilities of groups or countries in the area, the motivations and likely intentions of leaders, the interests and capabilities of other stakeholders, and what the potential threats are to U.S. interests and personnel both abroad and within the United States. The intelligence community also can provide assessments of the likely effects (near and long term) of proposed U.S. courses of action on specific individuals, groups, or national and regional populations. However, remember that policymakers may not always get all the information they want or feel that they need. The intelligence community is highly capable, but not omniscient.

An example of intelligence support to the interagency policy process is the National Counterterrorism Center. The NCTC is responsible for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism (CT), and conducting strategic operational planning by integrating all appropriate instruments of national power. As part of that last responsibility, the NCTC ensures that all elements of the Executive Branch—beyond just elements of the Intelligence Community—are coordinated in their counterterrorism efforts. The Director of the NCTC (D/NCTC) has two reporting channels. Regarding intelligence operations conducted by the intelligence community and NCTC’s intelligence analysis activities, the D/NCTC reports to the DNI. On matters
concerning the planning for strategic counterterrorism operations (other than wholly intelligence operations), the D/NCTC reports to the President.

Ultimately, it is up to the policy maker to decide how he or she uses intelligence; and there are many reasons why a policy maker will or will not use intelligence. For example, intelligence information enhances power in policy discussions when it bolsters one's own position, but, unfortunately, it may be discounted if it calls into question the wisdom of following a preferred policy path. Policymakers must work out how to resolve often-conflicting information or unknowns resulting from incomplete intelligence. For example, recent debates over national missile defense reflect differing interpretations of intelligence analyses about the technical capabilities and intentions of terrorist groups or states hostile to the United States. Policymakers may request analyses from specific intelligence agencies, or community-coordinated assessments produced under the authority of the National Intelligence Council. The NIC also produces National Intelligence Estimates (NIEs), typically at the request of policymakers, on strategic national security issues that make judgments about the course of future events and identify the implications for US national interests. Conversely, policymakers may resist additional intelligence analysis if they worry that their policy positions will not be supported by the results.

Although the intelligence community's mission is to produce objective analyses that support the policy process, it often is drawn into policy deliberations by providing assessments about the likely outcome of proposed courses of action, by determining what kinds of policies are most likely to influence leaders or groups, and by advising on whether different factions in foreign governments (including intelligence services) are likely to help or hinder the implementation of policies. The involvement of the Director of Central Intelligence George Tenet (July 1997-July 2004), with Israeli and Palestinian security services on security issues in a possible peace agreement reflects how intelligence sometimes has a direct involvement in the implementation of U.S. policy. If directed by the President, the Central Intelligence Agency also can be used to implement foreign policy through the use of covert action—secret activities in which the involvement of the United States is concealed and denied.

**Homeland Security**

Department of Homeland Security

The U.S. Department of Homeland Security (DHS) was formed on March 1, 2003, through the merger of over 22 programs and agencies (currently over 290,000 personnel) from throughout the Federal government. Headed by a cabinet-level Secretary of Homeland Security, DHS has a stated mission to lead "a concerted national effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive."79

To accomplish this mission, DHS has identified five responsibilities as part of the 2009 Quadrennial Homeland Security Review:80

1. Preventing Terrorism and Enhancing Security
   - Goal 1.1: Prevent Terrorist Attacks
   - Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities
   - Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership and Events

2. Securing and Managing our Borders
   - Goal 2.1: Effectively control U.S. Air, Land and Sea Borders
   - Goal 2.2: Safeguard Lawful Trade and Travel
   - Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations

3. Enforcing and Administering our Immigration Laws
   - Goal 3.1: Strengthen and Effectively Administer the Immigration System
   - Goal 3.2: Prevent Unlawful Immigration

4. Safeguarding and Securing Cyberspace
   - Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment
   - Goal 4.2: Promote Cybersecurity Knowledge and Innovation

5. Ensuring Resilience to Disasters
   - Goal 5.1: Mitigate Hazards
   - Goal 5.2: Enhance Preparedness
   - Goal 5.3: Ensure Effective Emergency Response
   - Goal 5.4: Rapidly Recover

DHS is charged with synthesizing and analyzing homeland security intelligence, assessing threats, guarding U.S. borders and airports, protecting the critical infrastructure of the country, and coordinating emergency response (including natural disaster assistance). The Department has broad responsibility for a wide range of functions and activities required to safeguard the citizens of
the United States, including coastal security, border security, customs, immigration, transportation security, infrastructure protection, emergency response, and information systems security. DHS’s intelligence mission includes analyzing and sharing information and intelligence pertinent to homeland security with State, local, tribal, territorial, and private sector partners, and other Intelligence Community members such as the Federal Bureau of Investigation (FBI), Director of National Intelligence (DNI), and the Central Intelligence Agency (CIA).

During 2006, DHS implemented a major reorganization based upon lessons learned from the operations of the Department since its inception. To fully perform its mission, DHS has three major "Directorates", seven operational Components, and 15 support Components (See Appendix I for a DHS organizational chart).\(^1\)

**Directorates**

- **Management (MGMT)** Directorate is responsible for Department budgets and appropriations, expenditure of funds, accounting and finance, procurement; human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. The Under Secretary for Management is assisted in carrying out management responsibilities and duties by a team that includes the following: Chief Administrative Services Officer; Chief Financial Officer; Chief Human Capital Officer; Chief Information Officer; Chief Procurement Officer; Chief Security Officer.

- **National Protection and Programs Directorate (NPPD)** seeks to advance the Department’s risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements. NPPD divisions include Federal Protective Service and the offices of Cyber Security and Communications, Infrastructure Protection, Risk Management and Analysis, and US-VISIT.

- **Science and Technology (S&T)** Directorate seeks to protect the homeland by providing Federal and local officials with state-of-the-art technology and other resources. S&T engages government, industry, and academia in collaborative efforts to identify and remedy areas of vulnerability through research, development, testing and evaluation of new technologies.

**DHS Operational Components**
- Federal Emergency Management Agency (FEMA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard (USCG)
- U.S. Customs and Border Protection (CBP)
- U.S. Immigration and Customs Enforcement (ICE)
• U.S. Secret Service (USSS)
• Transportation Security Administration (TSA)

Because of the overlapping issues between the global war on terrorism, homeland defense, and homeland security, DHS works closely with the Department of Defense’s (DOD) Assistant Secretary for Homeland Defense and with a number of DOD and other U.S. Government entities including USNORTHCOM as mentioned above in the section on the Department of Defense. In addition to working with DOD, DHS operates through its Under Secretary for Intelligence and Analysis (in her role as the Department’s Chief Intelligence Officer) on a daily basis with the DNI, CIA, FBI, and other elements of the Intelligence Community to coordinate the collection, analysis, and sharing of intelligence related to homeland security.

The reorganization of DHS in 2006 was intended to capitalize on the successful lessons learned during DHS’s brief existence, create new entities to more effectively coordinate the operations of the many Components of the agency, and improve strategic planning and policy coordination. Because of its broad responsibilities for homeland security, and its complex, multi-organizational structure, DHS has researched best practices in other departments and agencies, and developed structures and processes to more effectively manage its roles and missions. For example, like other agencies with responsibilities for national security operations, DHS staffs a 24-hour watch center (National Operations Center) for threat analysis and incident response. The Secretary of Homeland Security and senior advisors receive a daily security brief about developments, warning issues, policy concerns, and intelligence analysis. There are formalized procedures for working with IPCs, the National Security Staff, and responding to congressional inquiries and taskers. The DHS Office of the Executive Secretariat, in coordination with the Office of Policy, established a White House Actions and Interagency Coordination team which is designed to be a single point of contact for White House and interagency concerns and views, as well as ensuring that official DHS positions are coordinated and communicated through a single entity.

In addition to a formalized structure to support its participation in IPCs, DHS also has established standard operating procedures for supporting DHS participation at the HSC Deputies and Principals Committees level. These include staff work on interagency coordination and policy development, tasker identification, scheduling and briefing preparation, meeting participants and support, IPC developments, and preparation of meeting Summary of Conclusions (SOC).

In January 2011, the President approved PPD-7, National Terrorism Advisory System (NTAS), which directed the Secretary of Homeland Security to establish the NTAS. NTAS replaces the color-coded Homeland Security
Advisory System (HSAS), and the new system will more effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, and stakeholders in the private sector.

In coordination with other Federal entities, the Secretary of Homeland Security will decide whether an NTAS Alert should be issued after reviewing credible information about a terrorist threat. The alerts will include a clear statement that there is an imminent threat or elevated threat. NTAS Alerts will be based on the nature of the threat: in some cases, alerts will be sent directly to law enforcement or affected areas of the private sector, while in others, alerts will be issued more broadly to the American people through both official and media channels. NTAS Alerts contain a sunset provision indicating a specific date when the alert expires.

In addition to senior level policy development, coordination, and implementation, and defense against terrorist threats, DHS also must address preparations for responding to major emergencies within the U.S. According to Homeland Security Presidential Directive (HSPD) -5, "The Secretary of Homeland Security is the principal Federal official (PFO) for domestic incident management." As such, the DHS Secretary is "responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies." To coordinate the myriad federal, state, and local agencies that would be involved in a terrorist attack, major disaster or other homeland security "incident" is a daunting challenge for interagency cooperation and management. In response to this challenge, DHS may activate a strategic-level interagency Crisis Action Team to support execution of the Secretary of DHS' ability to execute his or her HSPD-5 responsibilities. When activated, the DHS Crisis Action Team will integrate its effort with DHS' National Operations Center to conduct its primary functions of strategic-level "situational awareness reporting, decision support, and planning activities" in support of the Secretary of DHS.

In the national security world of post 9/11, it is clear that the lines between traditional national security and homeland security increasingly have become blurred. The significant overlap of individuals who are members both of the National Security Council (NSC) and the HSC, the many overlapping issues handled by the respective PCs and DCs, and the many joint NSC-HSC IPCs all reflect the domestic nature of national security, and the many international facets of homeland security and defense. The highly complex aspects of trend analysis and interagency policy development, coordination, integration, implementation, and monitoring increasingly will continually test the ability of the many components of the U.S. Government and its senior policymakers to work together both across inter-departmental lines and international dimensions. The country and its national/homeland security apparatus must be capable of responding in innovative ways to new challenges that emerge and to ensure that
the myriad departments and agencies of the executive branch are able to work together effectively to advance U.S. national security efforts. Nothing less than the security of the United States of America is at stake.
**APPENDIX A**

**HISTORICAL NOMENCLATURE OF PRESIDENTIAL NATIONAL SECURITY POLICY DECISION DOCUMENTS**

<table>
<thead>
<tr>
<th>President</th>
<th>Type of Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truman</td>
<td>National Security Council papers (NSC)</td>
</tr>
<tr>
<td>Eisenhower</td>
<td>National Security Council papers (NSC)</td>
</tr>
<tr>
<td>Kennedy</td>
<td>National Security Action Memorandum (NSAM)</td>
</tr>
<tr>
<td>Johnson</td>
<td>National Security Action Memorandum (NSAM)</td>
</tr>
<tr>
<td>Nixon/Ford</td>
<td>National Security Decision Memorandum (NSDM)</td>
</tr>
<tr>
<td>Carter</td>
<td>Presidential Directive (PD)</td>
</tr>
<tr>
<td>Reagan</td>
<td>National Security Decision Directive (NSDD)</td>
</tr>
<tr>
<td>Bush</td>
<td>National Security Directive (NSD)</td>
</tr>
<tr>
<td>Clinton</td>
<td>Presidential Decision Directive (PDD)</td>
</tr>
<tr>
<td>Bush</td>
<td>National Security Presidential Directive (NSPD)</td>
</tr>
<tr>
<td>Obama</td>
<td>Presidential Policy Directive (PPD)(^85)</td>
</tr>
</tbody>
</table>

Note: Presidents use Executive Orders and PPDs (or their historical equivalents) to authorize most executive actions. In addition, the President uses directives called "findings" to authorize covert actions.
APPENDIX B

ASSISTANTS TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS

On March 23, 1953, President Dwight D. Eisenhower established the position of Assistant to the President for National Security Affairs. The following is a list of the people who have occupied this position:

<table>
<thead>
<tr>
<th>Name</th>
<th>Appointed</th>
<th>Departed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Cutler</td>
<td>March 23, 1953</td>
<td>April 2, 1955</td>
</tr>
<tr>
<td>Dillon Anderson</td>
<td>April 2, 1955</td>
<td>September 1, 1956</td>
</tr>
<tr>
<td>Robert Cutler</td>
<td>January 7, 1957</td>
<td>June 24, 1958</td>
</tr>
<tr>
<td>Gordon Gray</td>
<td>June 24, 1958</td>
<td>January 13, 1961</td>
</tr>
<tr>
<td>McGeorge Bundy</td>
<td>January 20, 1961</td>
<td>February 28, 1966</td>
</tr>
<tr>
<td>Walt W. Rostow</td>
<td>April 1, 1966</td>
<td>December 2, 1968</td>
</tr>
<tr>
<td>Henry A. Kissinger</td>
<td>December 2, 1968</td>
<td>November 3, 1975*</td>
</tr>
<tr>
<td>Brent Scowcroft</td>
<td>November 3, 1975</td>
<td>January 20, 1977</td>
</tr>
<tr>
<td>William P. Clark</td>
<td>January 4, 1982</td>
<td>October 17, 1983</td>
</tr>
<tr>
<td>Robert C. McFarlane</td>
<td>October 17, 1983</td>
<td>December 4, 1985</td>
</tr>
<tr>
<td>John M. Poindexter</td>
<td>December 4, 1985</td>
<td>November 25, 1986</td>
</tr>
<tr>
<td>Frank C. Carlucci</td>
<td>December 2, 1986</td>
<td>November 23, 1987</td>
</tr>
<tr>
<td>Brent Scowcroft</td>
<td>January 20, 1989</td>
<td>January 20, 1993</td>
</tr>
<tr>
<td>W. Anthony Lake</td>
<td>January 20, 1993</td>
<td>March 14, 1997</td>
</tr>
<tr>
<td>Samuel R. Berger</td>
<td>March 14, 1997</td>
<td>January 20, 2001</td>
</tr>
<tr>
<td>Condoleezza Rice</td>
<td>January 20, 2001</td>
<td>January 24, 2005</td>
</tr>
<tr>
<td>Stephen Hadley</td>
<td>January 25, 2005</td>
<td>January 19, 2009</td>
</tr>
<tr>
<td>James Jones</td>
<td>January 20, 2009</td>
<td>October 8, 2010</td>
</tr>
<tr>
<td>Thomas Donilon</td>
<td>October 8, 2010</td>
<td>to present</td>
</tr>
</tbody>
</table>

* Henry Kissinger served concurrently as Secretary of State from September 21, 1973 until November 3, 1975.
APPENDIX C

Obama Administration PPDs and PSDs

PPD 1 Organization of the National Security Council System (2/13/09)
PPD 2 Implementation of the National Strategy for Countering Biological Threats (11/23/09)
PPD 3 unavailable
PPD 4 National Space Policy (6/28/10)
PPD 5 unavailable
PPD 6 Global Development (9/22/10)
PPD 7 National Terrorism Advisory System (1/26/11)
PPD 8 National Preparedness (3/30/11)

PSD 1 Organizing for Homeland Security and Counterterrorism (2/23/09)
PSD 2 classified
PSD 3 National Space Policy Review (5/14/09)
PSD 4 2010 Nuclear Posture Review (5/21/09)
PSD 5 classified
PSD 6 2010 Quadrennial Defense Review (7/30/09)
PSD 7 U.S. Global Development Policy (8/13/09)
PSD 8 Export Control Reform (12/21/09)
PSD 9 Military Family Policy (5/11/10)
PSD 10 Creation of an Interagency Atrocities Prevention Board and Corresponding Interagency Review (8/4/11)
PSD 11 classified
U.S. Intelligence Community

Director of National Intelligence

National CounterTerrorism Center
National Intelligence Council
Intell Community Management

Program Managers

Central Intelligence Agency
Defense Intelligence Agency
FBI
National Geospatial Intelligence Agency
National Reconnaissance Office
National Security Agency

Departmental

Justice DEA
Dept of Energy Intell
Dept of Homeland Security Intelligence & Analysis
Dept of State Bureau of Intelligence & Research
Dept of Treasury Terrorism & Financial Intell

Services

Air Force Intell
Army Intell
Coast Guard Intell
Marine Corps Intell
Navy Intell
Appendix I:
ENDNOTES

3 The need to restructure the national security apparatus, in fact, had been long recognized. Between 1921 and 1945, 50 bills had been introduced into Congress to reorganize the War and Navy Departments. None was successful in being enacted into law.


24 During the early 1980's, the Reagan administration supported guerrillas (called "Contras") fighting against Nicaragua's Sandinista regime backed by Cuba and the Soviet Union. By 1984, the Democrat-controlled U.S. Congress had passed and strengthened the Boland Amendment which severely restricted U.S. financial support for the Contras. President Reagan instructed his National Security Advisor, Robert McFarlane, to find alternative means to support the Contra effort. Meanwhile, Iran was engaged in a bloody war of attrition with Iraq, and Tehran secretly approached the U.S. to obtain spare parts and weapons for its military forces. Despite a congressional embargo prohibiting arms sales to Iran because of the seizure of the U.S. embassy and its staff in 1979, and opposition from Secretary of State George Shultz and Secretary of Defense Caspar Weinberger, the White House (supported by CIA director William Casey) decided to sell weapons to Tehran both to generate funds to support the Contras, and to encourage the release of Americans still being held hostage by Iranian supported Muslim radicals in Lebanon. When a Lebanese magazine printed a story about the secret dealings in November 1986, the U.S. congress launched investigations and President Reagan appointed an independent inquiry committee chaired by former Senator John Tower and an independent counsel to investigate criminal wrongdoing. Fourteen people were indicted and six were convicted (most for conspiracy or lying to Congress). Later, President George H.W. Bush issued pardons to McFarlane, his successor ADM John Poindexter, two CIA officers, and Secretary of Defense Weinberger before his trial began.

25 See Report of the President's Special Review Board, U.S.


Retrieved July 2011. Federation of American Scientists website:
http://www.fas.org/irp/offdocs/direct.htm

27 Beginning in February 2002, the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence conducted a joint investigation into the activities of the U.S. Intelligence Community with regard to the September 11, 2001 attacks against the United States. The joint congressional investigation, entitled the Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001 or 'JIIICATAS911,' released its final report in December 2002. Concurrently, Congress and President Bush agreed to establish an independent bipartisan commission "to prepare a full and complete account of the circumstances" regarding the terrorist attacks of 9/11. Upon the enactment of Public Law 107-306 on November 27, 2002, the National Commission on Terrorist Attacks Upon the United States (more commonly known as the 9/11 Commission) was established. The commission released its final report in July 2004. For
additional information on the Joint Inquiry, see: http://www.gpoaccess.gov/serialset/creports/911.html. For additional information on the 9/11 Commission, see: http://govinfo.library.unt.edu/911/report/index.htm
31 Although called by a variety of names in past administrations, this most senior policy group below the National Security Council has been called the Principals Committee since the administration of George H.W. Bush (1989-1993).
34 These groups were called Interagency Working Groups (IWGs, pronounced "i-wigs") during the Clinton administration, Policy Coordination Committees, or PCCs, during the George W. Bush administration, and Interagency Policy Committees, or IPCs, by the Obama administration. Regardless of the name assigned, these working groups have shared similar responsibilities, functions, and seniority of participants in each administration.
35 The Executive Office of the President (EOP) was created in 1939 by President Franklin D. Roosevelt. The EOP is composed of senior advisory groups or offices established to advise the President across a range of critical policy areas and is overseen by the White House Chief of Staff. The following entities exist within the Executive Office of the President: National Security Council, National Economic Council, Council of Economic Advisers, Council on Environmental Quality, Domestic Policy Council, Office of Administration, Office of Management and Budget, Office of National Drug Control Policy, Office of Science and Technology Policy, Office of the United States Trade Representative, and the White House Office. Retrieved July 2011. White House website: http://www.whitehouse.gov/administration/eop

38 Within the Executive Office of the President, the most senior staff members have the title of Assistant to the President (such as the Assistant to the President for National Security Affairs—more commonly known as the National Security Advisor). Next in seniority on the staff are Deputy Assistants to the President. The third level of seniority are the Special Assistant to the President, who often also are the Senior Directors who manage the various regional and functional offices. The fourth level of seniority is Senior Directors who do not hold the title of Special Assistant to the President. Finally, the fifth level of substantive staff at the NSC hold the title of Director in regional or functional areas. NSC staff also may include "Special Advisors" who are responsible for areas of special concern to the President. See Appendix C for an organizational chart of the NSC staff.

39 The Obama White House has three APs (two of whom are DNSAs) and five DAPs (three of whom are DNSAs). The following positions utilize these titles:
Assistant to the President and National Security Advisor
Assistant to the President and Deputy National Security Advisor
Assistant to the President for Homeland Security and Counterterrorism (holds the rank of DNSA, but this designation is not used in his regular title)
Deputy Assistant to the President and National Security Staff Chief of Staff (holds the rank of DNSA, but this designation is not used in his regular title)
Deputy Assistant to the President and Deputy National Security Advisor for Strategic Communications and Speechwriting
Deputy Assistant to the President for International Economic Affairs
Deputy Assistant to the President for Homeland Security (not a DNSA)


SEC. 1004. OTHER FUNCTIONS AND ACTIVITIES.
    For the purpose of more effectively coordinating the policies and functions of the United States Government relating to homeland security, the Council shall—
(1) assess the objectives, commitments, and risks of the United States in the interest of homeland security and to make resulting recommendations to the President;
(2) oversee and review homeland security policies of the Federal Government and to make resulting recommendations to the President; and
(3) perform such other functions as the President may direct.

48 See Locher, James R., et al. Project on National Security Reform - Preliminary Findings. July 2008. For example, the Preliminary Findings report points out that President Carter provided few incentives to “compel” Secretary of State Cyrus Vance and National Security Advisor Zbigniew Brzezinski work together on the coordination of foreign policy development and execution (p. 15) and the experiences of other administrations in allocating responsibilities and authorities (p.45-47). During the George W. Bush administration, the intense involvement of the Departments of Defense and State in the global war on terrorism and missions in Afghanistan and Iraq resulted in Secretaries Rumsfeld and Powell being more frequently involved directly in policy development and coordination with the President and Vice President rather than coordinating policy through the NSA, Condoleezza Rice (author’s note). The PNSR also identifies a number of structural problems that often directly conflict with a president’s desire to delegate responsibility and authority to other parts of the interagency—frequently yielding less than satisfactory results and often leading to re-centralizing decision making and policy monitoring in the White House. See the “Systemic Deficiencies Burden The President With Issue Management” section on the Preliminary Findings report, pp. 45-52.
49 As amended.
50 See Presidential Policy Directive-1 (February 13, 2009).
For example, during the tenure of Condoleezza Rice as NSA for George W. Bush, she focused more on advising the President and ensuring coordination of policy between departments, and less on initiating policy at the NSC and directly monitoring the implementation of policy in Executive Branch departments. As the wars in Iraq, Afghanistan, and against terrorism progressed and more routine patterns of policy management were established, her successor, Stephen Hadley, increasingly focused upon brokering policy decisions and developing consensus between executive branch agencies. Hadley took a more hands-on approach to triage information coming into the NSC staff and organize the kinds of policy documents being prepared for the various policy committees and President Bush. President Obama’s first National Security Advisor, Gen (retired) James Jones, left such oversight to other members of the staff and focused more on maximizing the quality and range of information and policy options available to President Obama with detailed supporting information. Jones’ philosophy as the NSA also included placing a high priority on ensuring that President Obama always received multiple views on policy issues, and also received multiple options with regard to possible policy actions.

Managing communications as part of the policy process involves not only the President, but also the NSA and NSS staff. For example, the terrorist attacks of 9/11 and operations in Afghanistan and Iraq highlighted critical White House needs for maintaining situational awareness and ensuring that the President has the most up-to-date information. At the time of 9/11, the White House possessed limited meeting space beyond the Situation Room, and limited facilities for teleconferencing and other multi-media communication and presentations. In response to these requirements, the Bush administration undertook an extensive renovation of the Situation Room complex on the ground floor of the West Wing during 2006-2007 to construct multiple conference rooms incorporating state of the art secure telecommunications, video and data displays. These conference facilities enable the President, Principals, Deputies, and NSS staff to securely video conference with officials around the world and across departments and agencies in Washington D.C. and the rest of the United States. See also, “The White House Museum: Situation Room.”


See “Readout of National Security Advisor Tom Donilon’s meeting with Secretary Clinton, Secretary Gates and Israeli Minister of Defense Barak”,

82


57 Primary support for summits dealing principally with economic issues are supported by the National Economic Council staff or a designated Assistant Secretary or Deputy Assistant Secretary of State responsible for the political-economic issues of the summit, but the NSC does take the lead on economic summits with a strong political component, such as the G8 summit meetings.


59 The Secure Video-Teleconference Service (or SVTS) system is an important tool for the President and his National Security Staff to manage crises and rapidly coordinate policy development and implementation across the interagency and with U.S. officials and military commanders overseas. The Obama administration’s preference to maximize face-to-face meetings on policy issues for Washington-based senior officials is a departure from the pattern which evolved during the second Bush term when approximately 50% of PC meetings were conducted using the SVTS.

60 For example, the terrorist attacks of September 11, 2001 and the subsequent military missions of Operation Enduring Freedom (Afghanistan) and Operation Iraqi Freedom produced a policy decision tempo that resulted in unusually frequent (compared with historically normal day-to-day operations) NSC and PC meetings during the George W. Bush administration. Due to the simultaneity of the missions in Afghanistan and Iraq, the evolving policies and operations related to the global war on terrorism (GWOT), and domestic policy concerns related to the establishment of the Department of Homeland Security and potential domestic terrorist threats, the NSC and PC found themselves meeting on a regular, frequently daily, basis during the first term of the Bush administration. The swiftness with which potential threats and circumstances could change, and the complex, multiple, and often overlapping or conflicting policy and operational issues required regular review of mission outcomes and their implications for
maintaining or altering related policy decisions. The rapid pace of developments combined with the extensive senior government experience of the PC members (Vice President Cheney as a former Secretary of Defense, Secretary Powell as a former National Security Advisor and Chairman of the Joint Chiefs of Staff, and Secretary Rumsfeld as a previous Secretary of Defense) meant that many policy problems were identified, assessed, and decided at the NSC or PC level rather than being delegated to the DC or PCCs to be staffed. Furthermore, the continual evolution of events in the field meant that PC decisions coordinated one day might then be modified in a discussion by a principal the next day with President Bush or in a departmental meeting because some new development had occurred. As such, members of the Deputies Committee (as well as NSC staffers and PCC members) often had to work hard to keep abreast of evolving policy decisions from the PC level, and strived to implement well-coordinated policies across departments and agencies. As the crisis response mode eased, more issues were able to be analyzed and policy recommendations developed at the PCC and DC level before being presented to the PC.

66 See Madeleine Albright, Madam Secretary (New York: Miramax Books, 2003)
For additional information about DOD's role in Civil Support, see JCS Joint Publication 3-28, "Civil Support," (14 September 2007) Retrieved September 2010. Federation of American Scientists website:

See NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2006, Pub. L. No. 109-163, 119 STAT. 3404 (2006). See section 908 which amended subsection (b) of section 151 of title 10, U.S. code regarding the responsibilities of the Chairman of the Joint Chiefs of Staff. The change designated the CJCS as a statutory advisor to the HSC as well as the NSC.


"POSSE COMITATUS ACT" (18 USC 1385): A criminal law passed in 1878 proscribing use of Army (later, Navy, Marines, and Air Force) personnel to execute the laws except where expressly authorized by Constitution or Congress. Limit on use of military for civilian law enforcement also applies to Navy by regulation. Dec '81 additional laws were enacted (codified 10 USC 371-78) clarifying permissible military assistance to civilian law enforcement agencies--including the Coast Guard--especially in combating drug smuggling into the United States. Posse Comitatus clarifications emphasize supportive and technical assistance (e.g., use of facilities, vessels, aircraft, intelligence, tech aid, surveillance, etc.) while generally prohibiting direct participation of DOD personnel in law enforcement (e.g., search, seizure, and arrests). Source: http://www.history.navy.mil/library/online/posse%20comit.htm and http://www.northcom.mil/About/history_education/posse.html retrieved July 2011 (original source prior to 2008: http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/PosseComitatus.html


See Quadrennial Homeland Security Review Report, February 2010:
http://www.dhs.gov/qhsr

The 2008 DHS Strategic Plan has not yet been revised by the Obama administration, and is still used as the basis for organizational vision and planning for the department. The 2008 plan identified Strategic Goals and Objectives for the department which have been redefined as department "Responsibilities" to the American people. See Department of Homeland Security.


83 Information in this section cites and draws upon briefings and material provided by Incident Management Section of the Department of Homeland Security’s Office of Operations Coordination, Operations Coordination Division, Future Operations Branch.


Charlie Savage and the NSC Lawyers Group

By John Bellinger Sunday, November 8, 2015, 11:25 AM

A key theme of Charlie Savage's new book is that the Obama Administration -- led by a President, Vice President, Secretary of State, and (for a time) National Security Advisor who were all lawyers -- has been marked by "lawyerliness" in its national security decisionmaking. He asserts that the Obama era has been "government by lawyer, methodical and precise -- sometimes to a fault." As one example, Charlie writes that, in order to avoid the errors it perceived in Bush Administration national security decisionmaking, "the Obama team revived the interagency national security lawyers group, a bureaucratic institution from the 1990s that the Bush-Cheney Administration had essentially dismantled." On this point, Charlie overstates the case. In fact, the NSC "lawyers group" continued to meet regularly throughout the Bush Administration to consider and develop consensus on numerous legal issues; unfortunately its processes were circumvented in some significant matters, especially in the first term. The Obama Administration does appear to have placed a greater emphasis on consensus among interagency lawyers in most cases, although as Charlie explains, the Obama Administration has also engaged in some irregular legal processes, such as the White House's overruling of OLC's interpretation of the War Powers Resolution and the exclusion of both OLC and the State Department Legal Adviser in the review of legal issues relating to the UBL raid.

The NSC "lawyers group" was officially created by President George H.W. Bush by National Security Directive 79 to review certain intelligence matters. As I understand it from my predecessors, the lawyers group met regularly throughout the Clinton Administration. When she became National Security Advisor, Condoleezza Rice decided to retain the lawyers group. When I was NSC Legal Adviser from 2001-2005, I chaired the lawyers group and continued to use it to review numerous national security legal issues, including intelligence operations and counterterrorism matters. For example, as described in the 9-11 Commission report, in the summer of 2001, the lawyers group developed and agreed on the legal basis to use an armed Predator to kill Bin Laden. The general counsels of State, CIA, and DoD were invited to lawyers group meetings, although in practice they were more often represented by one of their deputy general counsels; OLC was generally represented by a Deputy Assistant Attorney General or senior lawyer responsible for national security issues, and the JCS was represented by the Chairman's Legal Adviser.

Some senior Bush Administration officials (both policy officials and lawyers) were not comfortable with legal decisionmaking by interagency consensus, which they believed to be slow and insufficiently deferential to the legal responsibilities of individual agencies, including OLC.
(Secretary Rumsfeld, for example, had long been skeptical of NSC processes and preferred to receive legal advice from his own lawyers rather than from an interagency group.) As a result, especially on counterterrorism issues after 9-11, consequential legal decisions were made by smaller groups of interagency lawyers. For example, Jack Goldsmith describes in The Terror Presidency that after 9-11, senior lawyers from DoD, OLC, the White House Counsel’s Office, and the Vice President’s Office created an informal “War Council” that excluded lawyers from the State Department, CIA, NSC, and JCS. And as Charlie Savage notes, Secretary Rice describes in her memoirs how the executive order creating military commissions in 2001 was prepared without the knowledge of the State Department, the CIA, or the NSC staff. National security legal processes were generally more inclusive and consensus-based in the Bush Administration’s second term.

Although I understand the argument that each agency head should rely primarily on his or her own general counsel for legal advice rather than defer to an interagency group, this model often does not work well in practice on complex issues. When disagreements on legal issues emerge at meetings of NSC Deputies and Principals, these senior policy officials often waste valuable policy time trying to debate legal details; they inevitably turn to their lawyers to explain the agency legal positions and/or to work out their differences with the lawyers from other departments. In my experience, it is also does not work well to rely exclusively or predominantly on OLC for opinions on national security law issues, especially questions involving international law. National security decisionmaking can usually be conducted more efficiently if interagency lawyers have discussed the issues in advance and attempted to reach consensus. If consensus cannot be reached, an NSC Principal is free to express a different view, as informed by her or his general counsel. And OLC can be asked for a definitive interpretation of domestic statutes, if necessary.

Although the Obama Administration did not “revive” the interagency lawyers group, they do appear to have placed greater emphasis on reaching interagency legal consensus on most issues. Nonetheless, that general approach was not followed in important cases. As we have discussed extensively on this blog, it was unprecedented, and troubling, that the White House apparently ignored OLC’s interpretation of the term “hostilities” in the War Powers Resolution in the context of the Libya operation. And it was similarly quite surprising that both OLC and the State Department Legal Adviser were excluded from the Obama Administration’s review of the Bin Laden raid. Both Jack and Marty Lederman have addressed the exclusion of OLC, but I was equally if not more concerned by the exclusion of the Legal Adviser for an operation in Pakistan that raised numerous international law issues. Although the planned operation was understandably the government’s most closely guarded secret, the State Department Legal Adviser would have been best-positioned to advise on its consistency with international law and its impact on other countries.
Speech
Harold Hongju Koh
Legal Adviser, U.S. Department of State
Annual Meeting of the American Society of International Law
Washington, DC
March 25, 2010

Thank you, Dean Arean, for that very generous introduction, and very special thanks to my good friends President Lucy Reed and Executive Director Betsy Anderson for the extraordinary work you do with the American Society of International Law. It has been such a great joy in my new position to be able to collaborate with the Society on so many issues.

It is such a pleasure to be back here at the ASIL. I am embarrassed to confess that I have been a member of ASIL for more than 30 years, since my first year of law school, and coming to the annual meeting has always been a highlight of my year. As a young lawyer just out of law school I would come to the American Society meeting and stand in the hotel lobby gaping at all the famous international lawyers walking by; for international lawyers, that is as close as we get to watching the Hollywood stars stroll the red carpet at the Oscars! And last year at this time, when this meeting was held, I was still in the middle of my confirmation process. So under the arcane rules of that process, I was allowed to come here to be seen, but not heard. So it is a pleasure finally to be able to address all of you and to give you my perspective on the Obama Administration's approach to international law.

Let me start by bringing you special greetings from someone you already know.

As you saw, my client, Secretary Clinton very much wanted to be here in person, but as you see in the headlines, this week she has been called away to Mexico, to meeting visiting Pakistani dignitaries, to testify on Capitol Hill, and many other duties. As you can tell, she is very proud of the strong historical relationship between the American Society and the State Department, and she is determined to keep it strong. As the Secretary mentioned, I and another long time member of the Society, your former President Anne Marie Slaughter of the Policy Planning Staff join her every morning at her 8:45 am senior staff meeting, so the spirit of the American Society is very much in the room (and the smell of the Society as well, as I am usually there at that hour clutching my ASIL coffee mug!)

Since this is my first chance to address you as Legal Adviser, I thought I would speak to three issues. First, the nature of my job as Legal Adviser. Second, to discuss the strategic vision of international law that we in the Obama Administration are attempting to implement. Third and finally, to discuss particular issues that we have grappled with in our first year in a number of high-profile areas: the International Criminal Court, the Human Rights Council, and what I call The Law of 9/11: detentions, use of force, and prosecutions.

I. The Role of the Legal Adviser

First, my job. I have now been the Legal Adviser of the State Department for about nine months. This is a position I first heard of about 40 years ago, and it has struck me throughout my career as the most fascinating legal job in the U.S. Government. Now that I’ve actually been in the job for awhile, I have become even more convinced that that is true, for four reasons.

First, I have absolutely extraordinary colleagues at the Legal Adviser’s Office, which we call “L,” which is surely the greatest international law firm in the world. Its numbers include many current lawyers and alumni who are sitting here in the audience, and it is a training ground for America’s international lawyers (To prove that point, could I have a show of hands of how many of you in the audience have worked in L sometime during your careers?) Our 175 lawyers are spread over 24 offices, including four extraordinary career deputies and a Counselor of International Law, nearly all of whom are members of this Society and many of whom you will find speaking on the various panels throughout this Annual Meeting program.

Second, I have extraordinary clients and you just saw one, Secretary Hillary Clinton, who is a remarkably able lawyer. Of course, another client of mine, the President, is also an outstanding lawyer, as are both Deputy Secretaries, the Department’s Counselor, the Deputy Chief of Staff, and a host of Under Secretaries and Assistant Secretaries.

Third, each day we tackle extraordinarily fascinating legal questions. When I was a professor, I would spend a lot of time trying to think up exam questions. For those of you who are professors, this job literally presents you with a new exam question every single day. For example, I had never really thought about the question: “can you attach a panda?” Or the question, can Mu’ammar al-Gadhafi erect a tent in Englewood, New Jersey, notwithstanding a contrary local

http://www.state.gov/s/l/releases/remarks/139119.htm
10/17/2016

The Obama Administration and International Law

Fourth and finally, my position allows me to play extraordinary and varied roles. Some government lawyers have the privilege for example, of giving regular advice to a particularly prominent client or pleading particular cases before a particular court. But the Legal Adviser must shift back and forth constantly between four rich and varied roles: which I call counselor, conscience, defender of U.S. interests, and spokesperson for international law.

As Counselor, I mean obviously, that the Legal Adviser must play all the traditional functions of an agency general counsel, but with a twist. Like every in-house counsel’s office, we do buildings and acquisitions, but those buildings may well be in Afghanistan or Beijing. We review government contracts, but they may require contracting activities in Iraq or Pakistan. We review employment decisions, but with respect to employees with diplomatic and consular immunities or special visa problems.

But in addition to being counselors, we also serve as a conscience for the U.S. Government with regard to international law. The Legal Adviser, along with many others in policy as well as legal positions, offers opinions on both the wisdom and morality of proposed international actions. For it is the unique role of the Legal Adviser’s Office to coordinate and render authoritative legal advice for the State Department on international legal issues, or as Dick Bilder once put it, to “speak law to power.” In this role, the Legal Adviser must serve not only as a source of black letter advice to his clients, but more fundamentally, as a source of good judgment. That means that one of the most important roles of the Legal Adviser is to advise the Secretary when a policy option being proposed is “lawful but awful.” As Herman Pfeffer, one former Legal Adviser, put it: “You should never say no to your client when the law and your conscience say yes; but you should never, ever, say yes when your law and conscience say no.” And because my job is simply to provide the President and the Secretary of State with the very best legal advice that I can give them, I have felt little conflict with my past roles as a law professor, dean and human rights lawyer, because as my old professor, former legal adviser Abram Haynes, once put it: “There’s nothing wrong with a lawyer holding the United States to its own best standards and principles.”

A third role the Legal Adviser plays is defender of the United States interests in the many international fora in which the U.S. appears— the International Court of Justice, where I had the honor recently of appearing for the United States in the Kosovo case; the UN Compensation Commission; the Iran-US Claims Tribunal; NAFTA tribunals (where I was privileged to argue recently before a Chapter 11 tribunal in the Grand River case) – and we also appear regularly in US domestic litigation, usually as of counsel to the Department of Justice in a case such as the Supreme Court’s current case of Samaritan v. Yousuf, on which this Society held a panel this morning.

A fourth and final role for the Legal Adviser, and the reason I’m here tonight, is to act as a spokesperson for the US Government about why international law matters. Many people don’t understand why obeying our international commitments is both right and smart, and that is a message that this Administration, and I as Legal Adviser, are committed to spreading.

II. The Strategic Vision

That brings me to my second topic: what strategic vision of international law are we trying to implement? How does obeying international law advance U.S. foreign policy interests and strengthen America’s position of global leadership? Or to put it another way, with respect to international law, is this Administration really committed to what our President has famously called “change we can believe in”? Some, including a number of the panelists who have addressed this conference, have argued that there is really more continuity than change from the last administration to this one.

To them I would answer that, of course, in foreign policy, from administration to administration, there will always be more continuity than change; you simply cannot turn the ship of state 360 degrees from administration to administration every four to eight years, nor should you. But, I would argue—and these are the core of my remarks today—to say that is to understand the most important difference between this administration and the last: and that is with respect to its approach and attitude toward international law. The difference in that approach to international law I would argue is captured in an Emerging “Obama-Clinton Doctrine,” which is based on four commitments: to: 1. Principled Engagement; 2. Diplomacy as a Critical Element of Smart Power; 3. Strategic Multilateralism; and 4. the notion that Living Our Values Makes us Stronger and Safer, by Following Rules of Domestic and International Law; and Following Universal Standards, Not Double Standards.

As articulated by the President and Secretary Clinton, I believe the Obama/Clinton doctrine reflects these four core commitments. First, a Commitment to Principled Engagement: A powerful belief in the interdependence of the global community is a major theme for our President, whose father came from a Kenyan family and who as a child spent several years in Indonesia.

Second, a commitment to what Secretary Clinton calls “smart power”—a blend of principle and pragmatism” that makes “intelligent use of all means at our disposal,” including promotion of democracy, development, technology, and human rights and international law to place diplomacy at the vanguard of our foreign policy.

Third, a commitment to what some have called Strategic Multilateralism: the notion acknowledged by President Obama at Cairo, that the challenges of the twenty-first century “can’t be met by any one leader or any one nation” and must therefore be addressed by open dialogue and partnership by the United States with peoples and nations across traditional regional divides, “based on mutual interest and mutual respect” as well as acknowledgment of “the rights and responsibilities of [all] nations.”

http://www.state.gov/s/l/releases/remarks/139119.htm
And fourth and finally, a commitment to *living our values by respecting the rule of law*. As I said, both the President and Secretary Clinton are outstanding lawyers, and they understand that by imposing constraints on government action, law legitimates and gives credibility to governmental action. As the President emphasized forcefully in his National Archives speech and elsewhere, the American political system was founded on a vision of common humanity, universal rights and rule of law. Fidelity to [these] values* makes us stronger and safer. This also means *following universal standards, not double standards*. In his Nobel lecture at Oslo, President Obama affirmed that “[a]dhering to standards, international standards, strengthens those who do, and isolates those who don’t.” And in her December speech on a 21st Century human rights agenda, and again two weeks ago in introducing our annual human rights reports, Secretary Clinton reiterated that “a commitment to human rights starts with universal standards and with holding everyone accountable to those standards, including ourselves.”

Now in implementing this ambitious vision—this Obama-Clinton doctrine based on principled international engagement, smart power, strategic multilateralism, and the view that global leadership flows to those who live their values and obey the law and global standards—I am reminded of two stories.

The first, told by a former teammate is about the late Mickey Mantle of the American baseball team, the New York Yankees, who, having been told that he would not play the next day, went out and got totally drunk (as he was wont to do). The next day, he arrived at the ballpark, somewhat impaired, but in the late innings was unexpectedly called upon to pinch-hit. After staggering out to the field, he swung wildly at the first two pitches and missed by a mile. But on the third pitch, he hit a tremendous home run. And when he returned to the dugout, he spouted out at the wildly cheering crowd and confided to his teammates, “[t]hose people don’t know how hard that really was.”[1]

In much the same way, I learned that the making of U.S. foreign policy is infinitely harder than it looks from the ivory tower. Why? Because, as lawyers, we are accustomed to the relatively orderly world of law and litigation, which is based on a knowable and identifiable structure and sequence of events. The workload comes with courtroom deadlines, page limits and scheduled arguments. But if conducting litigation is like climbing a ladder, making foreign policy is much more like driving the roundabout near the Coliseum in Rome.

In this maze of bureaucratic politics, you are only one lawyer, and there is only so much that any one person can do. Collective government decision-making creates enormous coordination problems. We in the Legal Adviser’s Office are not the only lawyers in government: On any given issue, my office needs to reach consensus decisions with all of the other interested State Department bureaus, but our Department as a whole then needs to coordinate its positions not just with other government law offices, which include: our lawyer clients (POTUS/SecState/DepSecState); White House Lawyers (WHCounsel/NSC Legal Counsel/USTR General Counsel); DOJ Lawyers (OGC, Jt Staff, CoComs, Services, JAGs); DOJ Lawyers (OLC, OSG, Litigating Divisions-Civ, Crim, Oil, NSD); IC Lawyers (DNI, CIA); DHS Lawyers, not to mention lawyers in the Senate and House.

To make matters even more complex, we participate in a complicated web of legal processes within processes: the policy process, the clearance process, the interagency process, the legislative process; and once a U.S. position is developed, an intergovernmental lawyering process. So unlike academics, who are accustomed to being individualists, in government you are necessarily part of a team. One obvious corollary to this is that as one government lawyer, your views and the views of your client are not the only views that matter. As Walter Dellinger observed when he worked at OLC:

“[U]nlike an academic lawyer, an executive branch attorney may have an obligation to work within a tradition of reasoned, executive branch precedent, memorialized in formal written opinions. Lawyers in the executive branch have thought and written for decades about the President’s legal authority... When lawyers who are now [in my office] begin to research an issue, they are not expected to turn to what I might have written or said in a floor discussion at a law professors’ convention. They are expected to look to the previous opinions of the Attorneys General and of heads of this office to develop and refine the executive branch’s legal positions.”[2]

Now to say that is not to say that one administration cannot or should not reverse a previous administration’s legal positions. But what it does mean, as I noted at my confirmation hearings, is that government lawyers should begin with a presumption of stare decisis—that an existing interpretation of the Executive Branch should stand—unless after careful review, a considered reexamination of the text, structure, legislative or negotiating history, purpose and practice under the treaty or statute firmly convinces us that a change to the prior interpretation is warranted.

So that is what I mean when I say it’s harder than it looks. And as those listening who have served in government know, it is a lot harder to get from a good idea to the implementation of that idea than those outside the government can imagine.

That brings me to my second, shorter story: about two Irishmen walking down the road near Galway. One of them asks the other, "So how do you get to Dublin?" And the other answers, "I wouldn't start from here."

In the same way, given the chance, no one would have started with what we inherited: the worst recession since the Depression, with conflicts in Iraq, Afghanistan, against al-Qaeda. Add to this mix a difficult and divided political environment, which makes it very difficult to get 60 Senate votes for cloture, much less the 67 you would need for treaty ratification, and such thorny carryover issues as resuming international engagement, closing Guantanamo, not to mention tackling an array of new challenges brought to us by the 21st century: climate change, attendant shifts in the polar environment; cyber crime, aggression and terrorism, food security, and global health just to name a few. Just to round things out, throw in a 7.0 earthquake in Haiti, another earthquake in Chile, four feet of snow in Washington, and you might well say to yourselves, to coin a phrase, "I wouldn't start from here."

http://www.state.gov/s/l/releases/remarks/139119.htm
The Obama Administration and International Law

But that having been said, how have we played the hand we have been dealt? What legal challenges do we face? There are really five fields of law that have occupied most of my time: what I call the law of international justice and dispute resolution, the law of 9/11, the law of international agreements, the law of the State Department, and the law of globalization. Tonight I want to focus on the first two of these areas: the law of international justice and dispute resolution and the law of 9/11. For they best illustrate how we have tried to implement the four themes I have outlined: principled engagement, multilateralism, smart power, and living our values.

III. Current Legal Challenges

A. International Justice and Dispute Resolution

By international justice and dispute resolution, I refer to the U.S.’s renewed relationship to international tribunals and other international bodies. Let me address two of them: the International Criminal Court and the U.N. Human Rights Council. As President Obama recognized, “a new era of engagement has begun and renewed respect for international law and institutions is critical if we are to resume American leadership in a new global century.”

1. The International Criminal Court

With respect to the U.S. relationship to the ICC, let me report on my recent participation in the Resumed 8th Session of ICC Assembly of States Parties in New York, from which I have just returned. Last November, Ambassador-at-Large for War Crimes Stephen Rapp and I led an interagency delegation that resumed engagement with the Court by attending a meeting of the ICC Assembly of States Parties (ASP). This was the first time that the United States had attended such a meeting, and this week’s New York meeting continued that November session. As you know, the United States is not party to the Rome Statute, but we have attended these meetings as an observer. Our goal in November was to listen and learn, and by listening to gain a better understanding of the issues being considered by the ASP and of the workings of the International Criminal Court.

Significantly, although during the last decade the U.S. was largely absent from the ICC, our historic commitment to the cause of international justice has remained strong. As you all know, we have not been silent in the face of war crimes and crimes against humanity. As one of the vigorous supporters of the work of the ad hoc tribunals regarding the former Yugoslavia, Rwanda, Cambodia, Sierra Leone, and Lebanon, the United States has worked for decades, and we will continue to work, with other States to ensure accountability on behalf of victims of such crimes. But as some of those ad hoc war crimes tribunals enter their final years, the eyes of the world are increasingly turned toward the ICC. At the end of May, the United States will attend the ASP’s Review Conference in Kampala, Uganda. There are two key items on the agenda: stock-taking and aggression.

In the current situation where the Court has open investigations and prosecutions in relation to four situations, but has not yet concluded any trials, the stock-taking exercise is designed to address ways to strengthen the Court, and includes issues such as state cooperation; complementarity; effect on victims; peace and justice; and universality of membership. Even as a non-State party, the United States believes that it can be a valuable partner and ally in the cause of advancing international justice. The Obama Administration has been actively looking at ways that the U.S. can, consistent with U.S. law, assist the ICC in fulfilling its historic charge of providing justice to those who have endured crimes of epic savagery and scope. And as Ambassador Rapp announced in New York, we would like to meet with the Prosecutor at the ICC to examine whether there are specific ways that the United States might be able to support the particular prosecutions that already underway in the Democratic Republic of Congo, Sudan, Central African Republic, and Uganda.

But as for the second agenda item, the definition of the crime of aggression, the United States has a number of serious concerns and questions. The crime of aggression, which is a jus ad bellum crime based on acts committed by the state, fundamentally differs from the other three crimes under the Court’s jurisdiction — genocide, war crimes, and crimes against humanity—which are jus in bello crimes directed against particular individuals. In particular, we are concerned that adopting a definition of aggression at this point in the court’s history could divert the ICC from its core mission, and potentially politicize and weaken this young institution. Among the States Parties we found strongly held, yet divergent, views on many fundamental and unresolved questions.

First, there are questions raised by the terms of the definition itself, including the degree to which it may depart from customary international law of both the “crime of aggression” and the state “act of aggression.” This encompasses questions like what does it mean when the current draft definition requires that an act of aggression must be a “manifest” —as opposed to an “egregious” violation of the U.N. Charter?

A second question of who decides. The United States believes that investigation or prosecution of the crime of aggression should not take place absent a determination by the U.N. Security Council that aggression has occurred. The U.N. Charter confers on the Security Council the responsibility for determining when aggression has taken place. We are concerned by the confusion that might arise if more than one institution were legally empowered to make such a determination in the same case, especially since these bodies, under the current proposal, would be applying different definitions of aggression.

Third, there are questions about how such a crime would potentially affect the Court at this point in its development. For example, how would the still-maturing Court be affected if its prosecutor were mandated to investigate and prosecute this crime, which by its very nature, even if perfectly defined, would inevitably be seen as political—both by those who are charged, as well as by those who believe aggressors have been wrongly left uncharged? To what extent would the availability of such a charge place burdens on the prosecutor in every case, both those in which he chooses to charge aggression and those in which he does not? If you think of the Court as a wobbly bicycle that is finally starting to move forward, is this frankly more weight than the bicycle can bear?

Fourth, would adopting the crime of aggression at this time advance or hinder the key goals of the stock-taking exercise: promoting complementarity, cooperation, and universality? With respect to complementarity, how would this principle apply to a crime of aggression? Do we want national courts to pass judgment on public acts of foreign states that are elements of the crime of aggression? Would adding at this time a crime that would run against heads of state

http://www.state.gov/s/rls/reports/remarks/139119.htm

324
and senior leaders enhance or obstruct the prospects for state cooperation with the Court? And will moving to adopt this highly politicized crime at a time when there is genuine disagreement on such issues enhance the prospects for universal adherence to the Rome Statute?

All of these questions go to our ultimate concern: has a genuine consensus yet emerged to finalize a definition of the crime of aggression? What outcome in Kampala will truly strengthen the Court at this critical moment in its history? What we heard at the Resumed Session in New York is that no clear consensus has yet emerged on many of these questions. Because this is such a momentous decision for this institution, which would bring about such an organic change in the Court’s work, that we believe that we should leave no stone unturned in search of genuine consensus. And we look forward to discussing these important issues with as many States Parties and Non States Parties as possible between now and what we hope will be a successful Review Conference in Kampala.

2. Human Rights Council

In addition to reengaging with the ICC, the United States has also reengaged the U.N. Human Rights Council in Geneva. Along with my long time friend and colleague, Assistant Secretary of State for Democracy, Human Rights and Labor Michael Posner, who has my old job, and Assistant Secretary of State for International Organizations Esther Brimmer, I had the privilege of leading the first U.S. delegation to return to the Human Rights Council this past September.

You know the history: In March 2006, the U.N. General Assembly voted overwhelmingly to replace the flawed Human Rights Commission with this new body: the Human Rights Council. The last Administration participated actively in the negotiations in New York to reform the Commission, but ultimately voted against adoption of the UNGA resolution that created the HRC, and decided not to run for a seat.

The UNGA resolution that created the HRC made a number of important changes from the commission process: it created the Universal Periodic Review process, a mandatory process of self-examination and peer review that requires each U.N. member state to defend its own record before the HRC every four years. The Obama Administration would like our report to serve as a model for the world. Accordingly, we are preparing our first UPR report, which will be presented this November, with outreach sessions in an unprecedented interagency listening tour being conducted in about ten locations around the United States to hear about human rights concerns from civil society, community leaders, and tribal governments. Second, the HRC and its various subsidiary bodies and mechanisms meet far more frequently throughout the year than did the Commission, a pace that exhausts delegations. Third, the election criteria were revised. So while HRC membership still includes a number of authoritarian regimes that do not respect human rights, the election requirement of a majority of UNGA votes in often competitive elections has led to certain countries being defeated for membership and others declining to run for a seat. The rule that only one-third of membership (16 members) can convene a special session, has led to a disproportionate number of special sessions dedicated to criticism of Israel, which already is the only country with a permanent agenda item dedicated to examination of its human rights practices: an unbalanced focus that we have clearly and consistently criticized.

When the Obama Administration took office, we faced two choices with respect to the Human Rights Council: we could continue to stay away, and watch the flaws continue and possibly get worse, or we could engage and fight for better outcomes on human rights issues, even if they would not be easy to achieve. With the HRC, as with the ICC and other fora, we have chosen principled engagement and strategic multilateralism. While the institution is far from perfect, it is important and deserves the long-term commitment of the United States, and the United States must deploy its stature and moral authority to improve the U.N. human rights system where possible. This is a long-term effort, but one that we are committed to seeing through to success consistent with the basic goals of the Obama-Clinton doctrine: principled engagement and universality of human rights law. Our inaugural session as an HRC member in September saw some important successes, most notably the adoption by consensus of a freedom of expression resolution, which we co-sponsored with Egypt, that brought warring regional groups together and preserved the resolution as a vehicle to express firm support for freedom of speech and expression. This resolution was a way of implementing some of the themes in President Obama’s historic speech in Cairo, bridging geographic and cultural divides and dealing with global issues of discrimination and intolerance. We also joined country resolutions highlighting human rights situations in Burma, Somalia, Cambodia, and Honduras, and were able to take positions joined by other countries on several resolutions on which the United States previously would have been isolated, including ones on toxic waste and the financial crisis. The challenges in developing a body that fairly and even-handedly addresses human rights issues are significant, but we will continue to work toward that end.

At the March HRC session, which ends tomorrow, we have continued to pursue principled engagement by taking on a variety of initiatives at the HRC that seek to weaken protections on freedom of expression, in particular, the push of some Council Members to ban speech that "defames" religions, such as the Danish cartoons. At this session, we made supported a country resolution on Guinea and made significant progress in opposing the Organization of the Islamic Conference’s highly problematic “defamation of religions” resolution, even while continuing to deal with underlying concerns about religious intolerance.

B. The Law of 9/11

Let me focus the balance of my remarks on that aspect of my job that I call "The Law of 9/11." In this area, as in the other areas of our work, we believe, in the President's words, that "living our values doesn't make us weaker, it makes us safer and it makes us stronger."
The Obama Administration and International Law

We live in a time, when, as you know, the United States finds itself engaged in several armed conflicts. As the President has noted, one conflict, in Iraq, is winding down. He also reminded us that the conflict in Afghanistan is a "conflict that America did not seek, one in which we are joined by forty-three other countries...in an effort to defend ourselves and all nations from further attacks." In the conflict occurring in Afghanistan and elsewhere, we continue to fight the perpetrators of 9/11: a non-state actor, al-Qaeda (as well as the Taliban forces that harbored al-Qaeda).

Everyone here at this meeting is committed to international law. But as President Obama reminded us, "the world must remember that it was not simply international institutions -- not just treaties and declarations -- that brought stability to a post-World War II world... [T]he instruments of war do have a role to play in preserving the peace."

With this background, let me address a question on many of your minds: how has this Administration determined to conduct these armed conflicts and to defend our national security, consistent with its abiding commitment to international law? Let there be no doubt: the Obama Administration is firmly committed to complying with all applicable law, including the laws of war, in all aspects of these ongoing armed conflicts. As the President reaffirmed in his Nobel Prize Lecture, "where force is necessary, we have a moral and strategic interest in binding ourselves to certain rules of conduct... even as we confront a vicious adversary that abides by no rules... the United States of America must remain a standard bearer in the conduct of war. That is what makes us different from those whom we fight. That is the source of our strength." We in the Obama Administration have worked hard since we entered office to ensure that we conduct all aspects of these armed conflicts -- in particular, detention operations, targeting, and prosecution of terrorist suspects -- in a manner consistent not just with the applicable laws of war, but also with the Constitution and laws of the United States.

Let me say a word about each: detention, targeting, and prosecution.

1. Detention

With respect to detention, as you know, the last Administration's detention practices were widely criticized around the world, and as a private citizen, I was among the vocal critics of those practices. This Administration and I personally have spent much of the last year seeking to revise those practices to ensure their full compliance with domestic and international law, first, by unequivocally guaranteeing humane treatment for all individuals in U.S. custody as a result of armed conflict and second, by ensuring that all detained individuals are being held pursuant to lawful authorities.

a. Treatment

To ensure humane treatment, on his second full day in office, the President unequivocally banned the use of torture as an instrument of U.S. policy, a commitment that he has repeatedly reaffirmed in the months since. He directed that executive officials could no longer rely upon the Justice Department OLC opinions that had permitted practices that I consider to be torture and cruel treatment -- many of which he later disclosed publicly -- and he instructed that henceforth, all interrogations of detainees must be conducted in accordance with Common Article 3 of the Geneva Conventions and with the revised Army Field Manual. An interagency review of U.S. interrogation practices later advised -- and the President agreed -- that no techniques beyond those in the Army Field Manual (and traditional noncoercive FBI techniques) are necessary to conduct effective interrogations. That Interrogation and Transfer Task Force also issued a set of recommendations to help ensure that the United States will not transfer individuals to face torture. The President also revoked Executive Order 13440, which had interpreted particular provisions of Common Article 3, and restored the meaning of those provisions to the way they have traditionally been understood in international law. The President ordered CIA "black sites" closed and directed the Secretary of Defense to conduct an immediate review -- with two follow-up visits by a blue ribbon task force of former government officials -- to ensure that the conditions of detention at Guantanamo fully comply with Common Article 3 of the Geneva Conventions. Last December, I visited Guantanamo, a place I had visited several times over the last two decades, and I believe that the conditions I observed are humane and meet Geneva Conventions standards.

As you all know, also on his second full day in office, the President ordered Guantanamo closed, and his commitment to doing so has not wavered, even as closing Guantanamo has proven to be an arduous and painstaking process. Since the beginning of the Administration, through the work of my colleague Ambassador Dan Fried, we have transferred approximately 57 detainees to 22 different countries, of whom 33 were resettled in countries that are not the detainees' countries of origin. Our efforts continue on a daily basis. Just this week, five more detainees were transferred out of Guantanamo for resettlement. We are very grateful to those countries who have contributed to our efforts to close Guantanamo by resettling detainees; that list continues to grow as more and more countries see the positive changes we are making and wish to offer their support.

During the past year, we completed an exhaustive, rigorous, and collaborative interagency review of the status of the roughly 240 individuals detained at Guantanamo Bay when President Obama took office. The President's Executive Order placed responsibility for review of each Guantanamo detainee with six entities -- the Departments of Justice, State, Defense, and Homeland Security, the Office of the Director of National Intelligence (ODNI), and the Joint Chiefs of Staff -- to collect and consolidate from across the government all information concerning the detainees and to ensure that diplomatic, military, intelligence, homeland security, and law enforcement viewpoints would all be fully considered in the review process. This interagency task force, on which several State Department attorneys participated, painstakingly considered each and every Guantanamo detainee's case to assess whether the detainee could be transferred or repatriated consistently with national security, the interests of justice, and our policy not to transfer individuals to countries where they would likely face torture or persecution. The six entities ultimately reached unanimous agreement on the proper disposition of all detainees subject to review. As the President has made clear, this is not a one-time review; there will be "a thorough process of periodic review, so that any prolonged detention is carefully evaluated and justified."

Similarly, the Department of Defense has created new review procedures for individuals held at the detention facility in Parwan at Bagram airfield, Afghanistan, with increased representation for detainees, greater opportunities to present evidence, and more transparent proceedings. Outside organizations have begun to monitor these proceedings, and even some of the toughest critics have acknowledged the positive changes that have been made.

http://www.state.gov/s/l/releases/remarks/139119.htm
b. Legal Authority to Detain

Some have asked what legal basis we have for continuing to detain those held on Guantanamo and at Bagram. But as a matter of both international and domestic law, the legal framework is well-established. As a matter of international law, our detention operations rest on three legal foundations. First, we continue to fight a war of self-defense against an enemy that attacked us on September 11, 2001, and before, and that continues to undertake armed attacks against the United States. Second, in Afghanistan, we work as partners with a consenting host government. And third, the United Nations Security Council has, through a series of successive resolutions, authorized the use of "all necessary measures" by the NATO countries constituting the International Security Assistance Force (ISAF) to fulfill their mandate in Afghanistan. As a nation at war, we must comply with the laws of war, but detention of enemy belligerents to prevent them from returning to hostilities is a well-recognized feature of the conduct of armed conflict, as the drafters of Common Article 3 and Additional Protocol II recognized and as our own Supreme Court recognized in Hamdi v. Rumsfeld.

The federal courts have confirmed our legal authority to detain in the Guantanamo habeas cases, but the Administration is not asserting an unlimited detention authority. For example, with regard to individuals detained at Guantanamo, we explained in a March 13, 2009 habeas filing before the DC federal court—and repeatedly in habeas cases since—that we are resting our detention authority on a domestic statute—the 2001 Authorization for Use of Military Force (AUMF)—as informed by the principles of the laws of war. Our detention authority in Afghanistan comes from the same source.

In explaining this approach, let me note two important differences from the legal approach of the last Administration. First, as a matter of domestic law, the Obama Administration has not based its claim of authority to detain those at Gitmo and Bagram on the President's Article II authority as Commander-in-Chief. Instead, we have relied on legislative authority expressly granted to the President by Congress in the 2001 AUMF.

Second, unlike the last administration, as a matter of international law, this Administration has expressly acknowledged that international law informs the scope of our detention authority. Both in our internal decisions about specific Guantanamo detainees, and before the courts in habeas cases, we have interpreted the scope of detention authority authorized by Congress in the AUMF as informed by the laws of war. Those laws of war were designed primarily for traditional armed conflicts among states, not conflicts against a diffuse, difficult-to-identify terrorist enemy, therefore construing what is "necessary and appropriate" under the AUMF requires some "translation," or analogizing principles from the laws of war governing traditional international conflicts.

Some commentators have criticized our decision to detain certain individuals based on their membership in a non-state armed group. But as those of you who follow the Guantanamo habeas litigation know, we have defended this position based on the AUMF, as informed by the text, structure, and history of the Geneva Conventions and other sources of the laws of war. Moreover, while the various judges who have considered these arguments have taken issue with certain points, they have accepted the overall proposition that individuals who are part of an organized armed group like al-Qaeda can be subject to law of war detention for the duration of the current conflict. In sum, we have based our authority to detain not on conclusory labels, like "enemy combatant," but on whether the factual record in the particular case meets the legal standard. This includes, but is not limited to, whether an individual joined with or became part of al-Qaeda or Taliban forces or associated forces, which can be demonstrated by relevant evidence of formal or functional membership, which may include an oath of loyalty, training with al-Qaeda, or taking positions with enemy forces. Often these factors operate in combination. While we disagree with the International Committee of the Red Cross on some of the particulars, our general approach of looking at "functional" membership in an armed group has been endorsed not only by the federal courts, but also is consistent with the approach taken in the targeting context by the ICRC in its recent study on Direct Participation in Hostilities (DPH).

A final point: the Obama Administration has made clear both its goal not only of closing Guantanamo, but also of moving to shift detention responsibilities to the local governments in Iraq and Afghanistan. Last July, I visited the detention facilities in Afghanistan at Bagram, as well as Afghan detention facilities near Kabul, and I discussed the conditions at those facilities with both Afghan and U.S. military officials and representatives of the International Committee of the Red Cross. I was impressed by the efforts that the Department of Defense is making both to improve our ongoing operations and to prepare the Afghans for the day when we turn over responsibility for detention operations. This Fall, DOD created a joint task force led by a three-star admiral, Robert Harward, to bring new energy and focus to these efforts, and you can see evidence of his work in the rigorous implementation of our new detainee review procedures at Bagram, the increased transparency of these proceedings, and closer coordination with our Afghan partners in our detention operations.

In sum, with respect to both treatment and detainability, we believe that our detention practices comport with both domestic and international law.

B. Use of Force

In the same way, in all of our operations involving the use of force, including those in the armed conflict with al-Qaeda, the Taliban and associated forces, the Obama Administration is committed by word and deed to conducting ourselves in accordance with all applicable law. With respect to the subject of targeting, which has been much commented upon in the media and international legal circles, there are obviously limits to what I can say publicly. What I can say is that it is the considered view of this Administration—and it has certainly been my experience during my time as Legal Adviser—that U.S. targeting practices, including lethal operations conducted with the use of unmanned aerial vehicles, comply with all applicable law, including the laws of war.

http://www.state.gov/s/l/releases/remarks/139119.htm
The United States agrees that it must conform its actions to all applicable law. As I have explained, as a matter of international law, the United States is in an armed conflict with al-Qaeda, as well as the Taliban and associated forces, in response to the horrific 9/11 attacks, and may use force consistent with its inherent right to self-defense under international law. As a matter of domestic law, Congress authorized the use of all necessary and appropriate force through the 2001 Authorization for Use of Military Force (AUMF). These domestic and international legal authorities continue to this day.

As recent events have shown, al-Qaeda has not abandoned its intent to attack the United States, and indeed continues to attack us. Thus, in this ongoing armed conflict, the United States has the authority under international law, and the responsibility to its citizens, to use force, including lethal force, to defend itself, including by targeting persons such as high-level al-Qaeda leaders who are planning attacks. As you know, this is a conflict with an organized terrorist enemy that does not have conventional forces, but that plans and executes its attacks against us and our allies while hiding among civilian populations. That behavior simultaneously makes the application of international law more difficult and more critical for the protection of innocent civilians. Of course, whether a particular individual will be targeted in a particular location will depend upon considerations specific to each case, including those related to the imminence of the threat, the sovereignty of the other states involved, and the willingness and ability of those states to suppress the threat the target poses. In particular, this Administration has carefully reviewed the rules governing targeting operations to ensure that these operations are conducted consistently with law of war principles, including:

- First, the principle of distinction, which requires that attacks be limited to military objectives and that civilians or civilian objects shall not be the object of the attack; and
- Second, the principle of proportionality, which prohibits attacks that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, that would be excessive in relation to the concrete and direct military advantage anticipated.

In U.S. operations against al-Qaeda and its associated forces— including lethal operations conducted with the use of unmanned aerial vehicles— great care is taken to adhere to these principles in both planning and execution, to ensure that only legitimate objectives are targeted and that collateral damage is kept to a minimum.

Recently, a number of legal objections have been raised against U.S. targeting practices. While today is obviously not the occasion for a detailed legal opinion responding to each of these objections, let me briefly address four:

First, some have suggested that the very act of targeting a particular leader of an enemy force in an armed conflict must violate the laws of war. But individuals who are part of such an armed group are belligerents and, therefore, lawful targets under international law. During World War II, for example, American aviators tracked and shot down the airplane carrying the architect of the Japanese attack on Pearl Harbor, who was also the leader of enemy forces in the Battle of Midway. This was a lawful operation then, and would be if conducted today. Indeed, targeting particular individuals serves to narrow the focus when force is employed and to avoid broader harm to civilians and civilian objects.

Second, some have challenged the very use of advanced weapons systems, such as unmanned aerial vehicles, for lethal operations. But the rules that govern targeting do not turn on the type of weapon system used, and there is no prohibition under the laws of war on the use of technologically advanced weapons systems in armed conflict— such as pilotless aircraft or so-called smart bombs— so long as they are employed in conformity with applicable laws of war. Indeed, using such advanced technologies can ensure both that the best intelligence is available for planning operations, and that civilian casualties are minimized in carrying out such operations.

Third, some have argued that the use of lethal force against specific individuals fails to provide adequate process and thus constitutes unlawful extrajudicial killing. But a state that is engaged in an armed conflict or in legitimate self-defense is not required to provide targets with legal process before the state may use lethal force. Our procedures and practices for identifying lawful targets are extremely robust, and advanced technologies have helped to make our targeting even more precise. In my experience, the principles of distinction and proportionality that the United States applies are not just recited at meetings. They are implemented rigorously throughout the planning and execution of lethal operations to ensure that such operations are conducted in accordance with all applicable law.

Fourth and finally, some have argued that our targeting practices violate domestic law, in particular, the long-standing domestic ban on assassinations. But under domestic law, the use of lawful weapons systems— consistent with the applicable laws of war— for precision targeting of specific high-level belligerent leaders acting in self-defense or during an armed conflict is not unlawful, and hence does not constitute "assassination."

In sum, let me repeat: as in the area of detention operations, this Administration is committed to ensuring that the targeting practices that I have described are lawful.

C. Prosecutions:

The same goes, third and finally, for our policy of prosecutions. As the President made clear in his May 2009 National Archives speech, we have a national security interest in trying terrorists, either before Article III courts or military commissions, and in keeping the number of individuals detained under the laws of war low.
The Obama Administration and International Law

Obviously, the choice between Article III courts and military commissions must be made on a case-by-case basis, depending on the facts of each particular case. Many acts of terrorism committed in the context of an armed conflict can constitute both war crimes and violations of our Federal criminal law, and they can be prosecuted in either federal courts or military commissions. As the last Administration found, those who have violated American criminal laws can be successfully tried in federal courts, for example, Richard Reid, Zacarias Moussaoui, and a number of others.

With respect to the criminal justice system, to reiterate what Attorney General Holder recently explained, Article III prosecutions have proven to be remarkably effective in incapacitating terrorists. In 2009, there were more defendants charged with terrorism violations in federal court than in any year since 9/11. In February 2010, for example, Najibullah Zazi pleaded guilty in the Eastern District of New York to a three-count information charging him with conspiracy to use weapons of mass destruction, specifically explosives, against persons or property in the United States, conspiracy to commit murder in a foreign country, and provision of material support to al-Qaeda. We have also effectively used the criminal justice system to pursue those who have sought to commit terrorist acts overseas. On March 18, 2010, for example, David Headley pleaded guilty to a dozen terrorism charges in U.S. federal court in Chicago, admitting that he participated in planning the November 2008 terrorist attacks in Mumbai, India, as well as later planning to attack a Danish newspaper.

As the President noted in his National Archives speech, lawfully constituted military commissions are also appropriate venues for trying persons for violations of the laws of war. In 2009, with significant input from this Administration, the Military Commissions Act was amended, with important changes to address the defects in the previous Military Commissions Act of 2006, including the addition of a provision that renders inadmissible any statements taken as a result of cruel, inhuman or degrading treatment. The 2009 legislative reforms also require the government to disclose more potentially exculpatory information, restrict hearsay evidence, and generally require that statements of the accused be admitted only if they were provided voluntarily (with a carefully defined exception for battlefield statements).

IV. CONCLUSION

In closing, in the last year, this Administration has pursued principled engagement with the ICC and the Human Rights Council, and has reaffirmed its commitment to international law with respect to all three aspects of the armed conflicts in which we find ourselves: detention, targeting and prosecution. While these are not all we want to achieve, neither are they small accomplishments. As the President said in his Nobel Lecture, "I have reaffirmed America's commitment to abide by the Geneva Conventions. We lose ourselves when we compromise the very ideals that we fight to defend. And we honor ideals by upholding them not when it's easy, but when it is hard." As President Obama went on to say, even in this day and age war is sometimes justified, but "this truth", he said, "must coexist with another—that no matter how justified, war promises human tragedy. The soldier's courage and sacrifice is full of glory ... But war itself is never glorious, and we must never trumpet it as such. So part of our challenge is reconciling these two seemingly irreconcilable truths— that war is sometimes necessary, and war at some level is an expression of human folly.”

Although it is not always easy, I see my job as an international lawyer in this Administration as reconciling these truths around a thoroughgoing commitment to the rule of law. That is the commitment I made to the President and the Secretary when I took this job with an oath to uphold the Constitution and laws of the United States. That is a commitment that I make to myself every day that I am a government lawyer. And that is a commitment that I make to each of you, as a lawyer deeply committed—as we all are—to the goals and aspirations of this American Society of International Law.

Thank you.

State Department Legal Adviser Brian Egan’s Speech at ASIL

By Benjamin Wittes Friday, April 8, 2016, 8:36 AM

International Law, Legal Diplomacy, and the Counter-ISIL Campaign

Thank you to Lori, Mark, and ASIL for inviting me. I am truly honored and humbled to be here today.

I am here today to talk about some key international law aspects of the United States’ ongoing armed conflict against ISIL. In so doing, I am following in the footsteps of others who have gone to some lengths in recent years to explain our government’s positions on key aspects of the law of armed conflict. This includes, most prominently, President Obama in his 2013 speech at the National Defense University and his 2014 remarks at West Point. A number of Administration lawyers have also spoken on these topics, including my predecessor, Harold Hongju Koh; former Attorney General Holder; and former Defense Department General Counsels Jeh Johnson and Stephen Preston. The Defense Department’s promulgation of its Law of War Manual last year has also made a significant contribution to the public discourse on these issues.

Some have said, however, that our legal approach to the counter-ISIL conflict has been one of the “most discussed and least understood” topics of U.S. practice in recent years.

Thus, at the risk of disappointing you at the outset of this talk, I suspect and hope that much of what I will say today will not be surprising. I also hope, however, that these remarks will provide clarity and help you understand better the U.S. international law approach to these important and consequential operations.

International law matters a great deal in how we as a country approach counterterrorism operations. Prior to my confirmation, I served as a Deputy White House Counsel and Legal Adviser to the National Security Council for nearly three years. Based on my experience in that position, I can tell you that the President, a lawyer himself, and his national security team have been guided by international law in setting the strategy for counterterrorism operations against ISIL. I can attest personally that the President cares deeply about these issues, and that he goes to great lengths to be sure that he understands them.

To start from first principles—the United States complies with the international law of armed conflict in our military campaign against ISIL, as we do in all armed conflicts. We comply with the law of armed conflict because it is the international legal obligation of the United States; because we have a proud history of standing for the rule of law; because it is essential to building and maintaining our international coalition; because it enhances rather than compromises our military effectiveness; and because it is the right thing to do.
I do not mean to suggest that identifying and applying key international law principles to this fight is easy or without controversy. The United States is engaged in an armed conflict with a non-State actor that controls significant territory, in circumstances in which multiple States and non-State actors also have been engaging in military operations against this enemy, other groups, and each other for several years. These conflicts raise novel and difficult questions of international law that the United States is called to address literally on a daily basis in conducting operations.

Of course, international law is also vitally important to other States. And as the President’s counterterrorism strategy has prioritized the development of partnerships with those who share our interests, I submit that it is increasingly important for the United States to engage in what I will call legal diplomacy with those countries with which we partner, as well as those with which we may not see eye to eye. Our ability to engage and work with partners can and often does turn on international legal considerations. We want to work with partners who will comply with international law, and our partners expect the same from us. In this way, international law serves as a critical enabler of international cooperation and joint action on a full range of matters, from the mundane to those that hit the front pages, such as the Iran nuclear deal, efforts to promote peace in Syria, maritime claims in the South China Sea, data privacy, and surveillance.

I will address three topics in my remarks. First, I will attempt to explain in greater detail the United States’ international legal basis for using force against ISIL, and some of the key rules of the law of armed conflict that apply to our fight against ISIL. Second, I will address how law of armed conflict-related considerations arise in the context of “partnered” operations—an area in which legal diplomacy is particularly critical. Third, I will address the interplay between law and policy in the conduct of hostilities by the United States—specifically those undertaken under the Presidential Policy Guidance that the President signed on May 22, 2013, known as the “PPG.”

**Jus ad bellum**

I will begin with the United States’ international law justification for resorting to the use of force, or the *jus ad bellum*.

As I mentioned a few minutes ago, the United States’ armed conflict with ISIL is taking place in a complicated environment—one in which a non-State actor, ISIL, controls significant territory and where multiple States and non-State actors have been engaging in military operations against ISIL, other groups, and each other for several years. Unfortunately, this scenario is not unprecedented in today’s world. Iraq and Syria resemble other countries where multiple armed conflicts may be going on simultaneously—countries like Yemen and Libya.
In such complex circumstances, States can potentially find themselves in more than one armed conflict or with multiple legal bases for using force. This complexity is why it is all the more important that we are clear and systematic in our thinking through how jus ad bellum principles for resorting to force apply to our actions and what uses of force those principles permit.

The U.N. Charter identifies the key international law principles that must guide State behavior when considering whether to resort to the use of force. Article 2(4) of the U.N. Charter provides in relevant part that “[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.” Article 51 of the U.N. Charter, on the other hand, specifies that “[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs.” Thus, the U.N. Charter recognizes the inherent right to resort to force in individual or collective self-defense. Similarly, the Charter does not prohibit an otherwise lawful use of force when undertaken with the consent of the State upon whose territory the force is to be used.

As a matter of international law, the United States has relied on both consent and self-defense in its use of force against ISIL. Let’s start with ISIL’s ground offensive and capture of Iraqi territory in June 2014 and the resulting decision by the United States and other States to assist with a military response. Beginning in the summer of 2014, the United States’ actions in Iraq against ISIL have been premised on Iraq’s request for, and consent to, U.S. and coalition military action against ISIL on Iraq’s territory in order to help Iraq prosecute the armed conflict against the terrorist group.

Upon commencing air strikes against ISIL in Syria in September 2014, the United States submitted a letter to the U.N. Security Council explaining the international legal basis for our use of force in Syria in accordance with Article 51 of the U.N. Charter. As the letter explained, Iraq had made clear it was facing a serious threat of continuing attacks from ISIL coming out of safe havens in Syria and had requested that the United States lead international efforts to strike ISIL in Syria. Consistent with the inherent right of individual and collective self-defense, the United States initiated necessary and proportionate actions in Syria against ISIL. The letter also articulated the United States’ position that Syria was unable or unwilling to effectively confront the threat that ISIL posed to Iraq, the United States, and our partners and allies.

Thus, although the United States maintains an individual right of self-defense against ISIL, it has not relied solely on that international law basis in taking action against ISIL. In Iraq, U.S. operations against ISIL are conducted with Iraqi consent and in furtherance of Iraq’s own armed conflict against the group. And in Syria, U.S. operations against ISIL are conducted in individual self-defense and the collective self-defense of Iraq and other States.
To say a few more words about self-defense: First, the inherent right of individual and collective self-defense recognized in the U.N. Charter is not restricted to threats posed by States. Nor is the right of self-defense on the territory of another State against non-State actors, such as ISIL, something that developed after 9/11. To the contrary, for at least the past two hundred years, States have invoked the right of self-defense to justify taking action on the territory of another State against non-State actors. As but one example, the oft-cited Caroline incident involved the use of force by the United Kingdom in self-defense against a non-State actor located in the United States. Although the precise wording of the justification for the exercise of self-defense against non-State actors may have varied, the acceptance of this right has remained the same.

Under the jus ad bellum, a State may use force in the exercise of its inherent right of self-defense not only in response to armed attacks that have occurred, but also in response to imminent ones before they occur.

When considering whether an armed attack is imminent under the jus ad bellum for purposes of the initial use of force against a particular non-State actor, the United States analyzes a variety of factors, including those identified by Sir Daniel Bethlehem in the enumeration he set forth in the American Journal of International Law—the ASIL's own in-house publication—in 2012. These factors include the nature and immediacy of the threat; the probability of an attack; whether the anticipated attack is part of a concerted pattern of continuing armed activity; the likely scale of the attack and the injury, loss, or damage likely to result therefrom in the absence of mitigating action; and the likelihood that there will be other opportunities to undertake effective action in self-defense that may be expected to cause less serious collateral injury, loss, or damage. The absence of specific evidence of where an attack will take place or of the precise nature of an attack does not preclude a conclusion that an armed attack is imminent for purposes of the exercise of the right of self-defense, provided that there is a reasonable and objective basis for concluding that an armed attack is imminent.

In the view of the United States, once a State has lawfully resorted to force in self-defense against a particular armed group following an actual or imminent armed attack by that group, it is not necessary as a matter of international law to reassess whether an armed attack is imminent prior to every subsequent action taken against that group, provided that hostilities have not ended. Under the PPG, however, the concept of imminence plays an important role as a matter of policy in certain U.S. counterterrorism operations, even when it is not legally required.

I'd also like to say a few words on how State sovereignty and consent factor into the international legal analysis when considering the use of force. President Obama has made clear that "America cannot take strikes wherever we choose; our actions are bound by consultations with partners, and respect for state sovereignty." This is true of our
operations against ISIL as it has been true in our non-international armed conflict against alQa’ida and associated forces.

Indeed, under the jus ad bellum, the international legal basis for the resort to force in self-defense on another State’s territory takes into account State sovereignty. The international law of self-defense requires that such uses of force be necessary to address the threat giving rise to the right to use force in the first place. States therefore must consider whether unilateral actions in self-defense that would impinge on a territorial State’s sovereignty are necessary or whether it might be possible to secure the territorial State’s consent before using force on its territory against a non-State actor. In other words, international law not only requires a State to analyze whether it has a legal basis for the use of force against a particular non-State actor—which I’ll call the “against whom” question—but also requires a State to analyze whether it has a legal basis to use force against that non-State actor in a particular location—which I’ll call the “where” question.

It is with respect to this “where” question that international law requires that States must either determine that they have the relevant government’s consent or, if they must rely on self-defense to use force against a non-State actor on another State’s territory, determine that the territorial State is “unable or unwilling” to address the threat posed by the non-State actor on its territory. In practice, States generally rely on the consent of the relevant government in conducting operations against ISIL or other non-State actors even when they may also have a self-defense basis to use force against those non-State actors, and this consent often takes the form of a request for assistance from a government that is itself engaged in an armed conflict against the relevant group. This is the case with respect to ISIL in Iraq.

Of course, the concept of consent can pose challenges in a world in which governments are rapidly changing, or have lost control of significant parts of their territory, or have shown no desire to address the threat. Thus, it sometimes can be a complex matter to identify the appropriate person or entity from whom consent should be sought. The U.S. Government carefully considers these issues when considering the question of consent.

In some cases, international law does not require a State to obtain the consent of the State on whose territory force will be used. In particular, there will be cases in which there is a reasonable and objective basis for concluding that the territorial State is unwilling or unable to effectively confront the non-State actor in its territory so that it is necessary to act in self-defense against the non-State actor in that State’s territory without the territorial State’s consent. For example, in the case of ISIL in Syria, as indicated in our Article 51 letter, we could act in self-defense without Syrian consent because we had determined that the Syrian regime was unable or unwilling to prevent the use of its territory for armed attacks by ISIL. This “unable or unwilling” standard is, in our view, an important application of the requirement that a State, when relying on self-defense for its use of force in another
State's territory, may resort to force only if it is necessary to do so—that is, if measures short of force have been exhausted or are inadequate to address the threat posed by the non-State actor emanating from the territory of another State.

The unable or unwilling standard is not a license to wage war globally or to disregard the borders and territorial integrity of other States. Indeed, this legal standard does not dispense with the importance of respecting the sovereignty of other States. To the contrary, applying the standard ensures that the sovereignty of other States is respected. Specifically, applying the standard ensures that force is used on foreign territory without consent only in those exceptional circumstances in which a State cannot or will not take effective measures to confront a non-State actor that is using its territory as a base for attacks and related operations against other States.

With respect to the “unable” prong of the standard, inability perhaps can be demonstrated most plainly, for example, where a State has lost or abandoned effective control over the portion of its territory from which the non-State actor is operating. This is the case with respect to the situation in Syria. By September 2014, the Syrian government had lost effective control of much of eastern and northeastern Syria, with much of that territory under ISIL’s control.

**Jus in bello**

In the next few minutes I’d like to shed some light on the jus in bello—the legal rules we follow in carrying out the fight against ISIL. As a threshold matter, some of our foreign partners have asked us how we classify the conflict with ISIL and thus what set of rules applies. Because we are engaged in an armed conflict against a non-State actor, our war against ISIL is a non-international armed conflict, or NIAC. Therefore, the applicable international legal regime governing our military operations is the law of armed conflict covering NIACs, most importantly, Common Article 3 of the 1949 Geneva Conventions and other treaty and customary international law rules governing the conduct of hostilities in noninternational armed conflicts.

The rules applicable in NIACs have received close scrutiny since the September 11 attacks within the U.S. Government, in our courts in the context of ongoing litigation concerning detention and military commission prosecutions, and in the expanding and ever more sophisticated treatment that these issues receive in academia.

I would like to clarify briefly some of the rules that the United States is bound to comply with as a matter of international law in the conduct of hostilities during NIACs. In particular, I’d like to spend a few minutes walking through some of the targeting rules that the United States regards as customary international law applicable to all parties in a NIAC:
-- First, parties must distinguish between military objectives, including combatants, on the one hand, and civilians and civilian objects on the other. Only military objectives, including combatants, may be made the object of attack.

-- Insofar as objects are concerned, military objectives are those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. The United States has interpreted this definition to include objects that make an effective contribution to the enemy's war-fighting or war-sustaining capabilities.

-- Feasible precautions must be taken in conducting an attack to reduce the risk of harm to civilians, such as, in certain circumstances, warnings to civilians before bombardments.

-- Customary international law also specifically prohibits a number of targeting measures in NIACs. First, attacks directed against civilians or civilian objects as such are prohibited. Additionally, indiscriminate attacks, including but not limited to attacks using inherently indiscriminate weapons, are prohibited.

-- Attacks directed against specifically protected objects such as cultural property and hospitals are also prohibited unless their protection has been forfeited.

-- Also prohibited are attacks that violate the principle of proportionality – that is, attacks against combatants or other military objectives that are expected to cause incidental harm to civilians that would be excessive in relation to the concrete and direct military advantage anticipated.

-- Moreover, acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.

To elaborate further and correct some possible misunderstandings regarding who the United States targets as an enemy in its ongoing armed conflicts, I'd like to explain how the United States assesses whether a specific individual may be made the object of attack.

In many cases we are dealing with an enemy who does not wear uniforms or otherwise seek to distinguish itself from the civilian population. In these circumstances, we look to all available real-time and historical information to determine whether a potential target would be a lawful object of attack. To emphasize a point that we have made previously, it is not the case that all adult males in the vicinity of a target are deemed combatants. Among other things, the United States may consider certain operational activities, characteristics, and identifiers when determining whether an individual is taking a direct part in hostilities or whether the individual may formally or functionally be considered a member of an
organized armed group with which we are engaged in an armed conflict. For example, with respect to membership in an organized armed group, we may examine the extent to which the individual performs functions for the benefit of the group that are analogous to those traditionally performed by members of State militaries that are liable to attack; is carrying out or giving orders to others within the group to perform such functions; or has undertaken certain acts that reliably indicate meaningful integration into the group.

Partnerships and legal diplomacy

I'd like to turn next to discussing the international coalitions and other partnerships that are critical to the fight against ISIL and the legal diplomacy that helps facilitate and sustain those partnerships. Sixty-six partners are engaged as part of the coalition that is steadily degrading ISIL. In the course of building and maintaining that strong coalition, we have also sought to navigate legal differences and find common legal ground. Some of our allies and partners have different international legal obligations because of the different treaties to which they are party, and others may hold different legal interpretations of our common obligations. Legal diplomacy plays a key role in building and maintaining the counterISIL military coalition and fostering interoperability between its members. Legal diplomacy builds on common understandings of international law, while also seeking to bridge or manage the specific differences in any particular State's international obligations or interpretations.

Public explanations of legal positions are an important part of legal diplomacy. The United States is not alone in providing such public explanations. Over the last 18 months, for example, nine of our coalition partners have submitted public Article 51 notifications to the U.N. Security Council explaining and justifying their military actions in Syria against ISIL. Though the exact formulations vary from letter to letter, the consistent theme throughout these reports to the Security Council is that the right of self-defense extends to using force to respond to actual or imminent armed attacks by non-State armed groups like ISIL. Those States' military actions against ISIL in Syria and their public notifications are perhaps the clearest evidence of this understanding of the international law of self-defense.

More frequently, however, it is through private consultations that governments seek to understand each other's legal rationale for military operations. These private discussions help frame the public conversation on some of the central legal issues, and they are crucial to securing the vital cooperation of partners who want to understand our legal basis for acting. For example, there are times when the United States has sought the assistance of key allies in taking direct action against terrorist targets, but before these allies would aid us, the lawyers in their foreign ministries have sought a better understanding of the legal basis for our operations. The prompt, compelling, and – at times – very early morning explanations provided by our attorneys can be crucial to enabling such operations.
These conversations also go the other way. The U.S. commitment to upholding the law of armed conflict also extends to promoting law of armed conflict compliance by our partners. In the campaign against ISIL and beyond, coalitions and partnerships with other States and non-State actors are increasingly prominent features of current U.S. military operations. When others seek our assistance with military operations, we ensure that we understand their legal basis for acting. We also take a variety of measures to help our partners comply with the law of armed conflict and to avoid facilitating violations through our assistance. Examples of such measures include vetting and training recipients of our assistance and monitoring how our assistance is used.

Some have argued that the obligation in Common Article 1 of the Geneva Conventions to "ensure respect" for the Conventions legally requires us to undertake such steps and more vis-à-vis not only our partners, but all States and non-State actors engaged in armed conflict. Although we do not share this expansive interpretation of Common Article 1, as a matter of policy, we always seek to promote adherence to the law of armed conflict generally and encourage other States to do the same. As a matter of international law, we would look to the law of State responsibility and our partners’ compliance with the law of armed conflict in assessing the lawfulness of our assistance to, and joint operations with, those military partners.

Law and Policy

Finally, I’d like to touch on the interplay between law and policy when the United States takes lethal action in armed conflicts and how the United States often applies policy standards that exceed what the law of armed conflict requires.

As a matter of international law, the United States is bound to adhere to the law of armed conflict. In many cases, the United States imposes standards on its direct action operations that go beyond the requirements of the law of armed conflict. For example, the U.S. military may impose an upper limit as a matter of policy on the anticipated number of non-combatant casualties that is much lower than that which would be lawful under the rule that prohibits attacks that are expected to cause excessive incidental harm.

Additionally, although the United States is not a party to the 1977 Additional Protocol II to the 1949 Geneva Conventions and therefore not bound to comply with its provisions as a matter of treaty law, current U.S. practice is already consistent with the Protocol’s provisions, which provide rules applicable to States parties in non-international armed conflict. This is a treaty that the Reagan Administration submitted to the Senate for its advice and consent to ratification, and every subsequent Administration has continued that support.

I’d like to focus my comments over the next few minutes on U.S. operations to capture or employ lethal force against terrorist targets outside areas of active hostilities. In addition to
the law of armed conflict, these operations are governed by policy guidance issued by the President in 2013. This policy guidance, known as the PPG, reflects this Administration’s efforts to strengthen and refine the process for reviewing and approving counterterrorism operations outside of the United States and “areas of active hostilities.” The phrase “areas of active hostilities” is not a legal term of art—it is a term specific to the PPG. For the purpose of the PPG, the determination that a region is an “area of active hostilities” takes into account, among other things, the scope and intensity of the fighting. The Administration currently considers Afghanistan, Iraq, and Syria to be “areas of active hostilities,” which means that the PPG does not apply to operations in those States.

Substantively, the PPG imposes certain heightened policy standards that exceed the requirements of the law of armed conflict for lethal targeting. The President has done so out of a belief that implementing such heightened standards outside of hot battlefields is the right approach to using force to meet U.S. counterterrorism objectives and protect American lives consistent with our values.

Of course, the President always retains authority to take lethal action consistent with the law of armed conflict, even if the PPG’s heightened policy standards may not be met. But in every case in which the United States takes military action, whether in or outside an area of active hostilities, we are bound to adhere as a matter of international law to the law of armed conflict. This includes, among other things, adherence to the fundamental law of armed conflict principles of distinction, proportionality, necessity, and humanity.

The Administration has already identified a number of the aspects in which the PPG imposes policy standards for the use of lethal force in counterterrorism operations that go beyond the requirements of the law of armed conflict. I’d like to focus on one key aspect here. The PPG establishes measures that go beyond the law of armed conflict in order to minimize risks to civilians to the greatest extent possible. In particular, the PPG establishes a threshold of “near certainty” that non-combatants will not be injured or killed. This standard is also higher than that imposed by the law of armed conflict, which contemplates that civilians will inevitably and tragically be killed in armed conflict.

In addition, with respect to lethal action, the PPG generally requires an assessment that capture of the targeted individual is not feasible at the time of the operation. The law of armed conflict does not itself impose any such “least restrictive means” obligation; instead, combatants may be targeted with lethal force at any time, provided that they are not “out of the fight” due to capture, surrender, illness, or injury.

I hope that this discussion of the PPG and other distinctions between law and policy has given you an understanding not only of the difference between the legal and policy constraints on U.S. lethal targeting, but also better appreciation of the lengths this
government goes to in order to minimize harm to civilians outside of hot battlefields while also taking the direct action necessary to protect the United States, our partners, and allies.

**Conclusion**

In closing, I’ll speak to a final aspect of legal diplomacy, one which my predecessors have emphasized in their public remarks as well. As Legal Adviser, one of my roles is to serve as a spokesperson for the U.S. Government on the importance and relevance of international law, and how the U.S. Government interprets, applies, and complies with international law. Part of our legal diplomacy is carried out with our foreign counterparts behind closed doors. But public legal diplomacy is a critical aspect of our work as well, as my predecessors—several of whom are in the audience today—have ably demonstrated.

It is not enough that we act lawfully or regard ourselves as being in the right. It is important that our actions be understood as lawful by others both at home and abroad in order to show respect for the rule of law and promote it more broadly, while also cultivating partnerships and building coalitions. Even if other governments or populations do not agree with our precise legal theories or conclusions, we must be able to demonstrate to others that our most consequential national security and foreign policy decisions are guided by a principled understanding and application of international law.

I hope that I have succeeded in providing some clarity today on the United States’ approach to international law in the counter-ISIL campaign. I am confident, however, that I have not answered all of your questions. We will seek opportunities to provide additional clarity on these issues in the months ahead. In the meantime, I have reserved the remainder of my time for questions. Thank you.

**Topics:** International Law

**Tags:** Brian Egan

Benjamin Wittes is editor in chief of Lawfare and a Senior Fellow in Governance Studies at the Brookings Institution. He is the author of several books and is co-chair of the Hoover Institution’s Working Group on National Security, Technology, and Law.

@benjaminwittes

341
Contents

Introduction .......................................................................................................................... 1
The Strategic Context Leading to the Goldwater-Nichols Act .............................................. 2
  DOD Challenges Prosecuting Joint Operations ................................................................. 2
  Desert One, 1980 ............................................................................................................. 3
  Grenada, 1983 .................................................................................................................. 4
  Beirut, 1983 ..................................................................................................................... 5
The Goldwater-Nichols Legislation ...................................................................................... 6
  Contents of the Act ......................................................................................................... 7
  Evaluations of the Goldwater-Nichols Legislation ............................................................ 8
The Strategic Context in 2016 ........................................................................................... 10
Emerging Threats .............................................................................................................. 10
The Fiscal Challenge ......................................................................................................... 11
Why Reform DOD Today? ................................................................................................. 13
The Defense Management and Reform Challenge .......................................................... 14
  Conceptualizing DOD’s Enterprise-Level Functions ......................................................... 15
  Efficiency vs. Effectiveness ......................................................................................... 16
  Headquarters Reductions ............................................................................................... 17
Framing the Problem: Current DOD Reform Concepts .................................................. 20
Current Defense Reform Proposals ................................................................................... 23
  External Defense Expert Reform Proposals .................................................................. 24
    Formulating Requirements ......................................................................................... 24
    Managing Costs ........................................................................................................ 26
    Building Capabilities .............................................................................................. 27
    Interagency Reform ................................................................................................. 28
  The Pentagon’s View on Reform Proposals .................................................................. 28
    Formulating Requirements ......................................................................................... 29
    Managing Costs ........................................................................................................ 31
    Building Capabilities .............................................................................................. 32
Recent Legislation on Defense Reform ............................................................................ 34
Issues for Congress .......................................................................................................... 42

Figures

Figure 1. DOD Enterprise-Level Management .................................................................. 16

Tables

Table 1. Select DOD Reform Proposals ............................................................................ 35

Appendixes

Appendix. Select Defense Management and Organizational Reform Proposals since the
  1980s ............................................................................................................................... 44
Contacts

Author Contact Information ........................................................................................................ 60
Introduction


Among defense scholars, observers, and practitioners there has been a near-constant drumbeat to reform one aspect or another of the DOD since its inception in 1947.\footnote{The 1947 Act actually established the “National Military Establishment” with a weak Secretary of Defense (SecDef). This was revised in 1949 to strengthen the Secretary, reduce the roles of service secretaries, ensure that SecDef he was the principal advisor to the President on matters of national security, and renamed the NME to the Department of Defense. See for more details on reform initiatives after the end of the Cold War.} Most observers agree that after 30 years, a comprehensive review of the Goldwater-Nichols legislation is warranted.\footnote{See, for example: CRS Recorded Event WRE00135, Defense Acquisition Reform: Is It Time for Another Goldwater-Nichols?, by Moshe Schwartz.} Further, there appears to be a broad consensus among observers that DOD must retain its strength while becoming considerably more agile in order to enable the United States to meet a variety of critical national security challenges.\footnote{See, for example, Center for Strategic and International Studies, Video: Defense Reform in the 21st Century: Guiding Principles for Reform Panel Discussion, March 14, 2016, http://cssis.org/multimedia/video-defense-reform-21st-century; Chairman Mac Thornberry, Speech to the National Press Club, January 16, 2016.}

Yet agreement seemingly ends there. There appears to be little consensus regarding what changes are needed within DOD and what specific direction reform ought to take. Discussions have begun to coalesce around a number of proposals, including reforming defense acquisition processes, further strengthening the Joint Staff, reducing Pentagon staffs, and better empowering the services in the “joint” arena. However, ideas vary on how, specifically, to accomplish those goals. Disagreement also exists as to whether or not reorganizing DOD alone will be sufficient. Some observers maintain that a reform of the broader interagency system on national security matters is needed.\footnote{See, for example, the Project on National Security Reform, http://www.pnsr.org/; Clark A. Murdock and Michele A. (continued...)}
This lack of consensus appears to result from diverging ideas as to what are the key challenges with the way DOD—and the national security architecture more broadly—is organized and operates. The variety of views reflects the complexity of these institutions. One observer refers to the present DOD reform debate as akin to a “Rorschach test,” noting that defense experts tend to diagnose what they believe to be critical national security challenges based on their own experiences and priorities. Without a common understanding of the root causes of these organizational frictions, solutions to the national security organization challenge differ considerably. The complex nature of the Pentagon and national security bureaucracies adds to the many challenges of DOD management reform.

Despite these obstacles, the case for reforming the Department of Defense is gaining traction among observers. The international security environment has grown ever more complex, in manners unforeseen when the Goldwater-Nichols legislation was enacted. This report is designed to assist Congress as it evaluates the many different defense reform proposals suggested by the variety of stakeholders and institutions within the U.S. national security community. It includes an outline of the strategic context for defense reform, both in the Goldwater-Nichols era and today. It then builds a framework to understand the DOD management challenge, and situates some of the most-discussed reform proposals within that framework. It concludes with some questions Congress may ponder as it exercises oversight over the Pentagon.

The Strategic Context Leading to the Goldwater-Nichols Act

The changes that the Goldwater-Nichols legislation made to the Department of Defense, and in particular, the way that DOD conducts military operations, are in many ways central to how the Department conducts military operations today. Indeed, many organization design decisions that were taken—in particular, clarifying the chain of command for more effective prosecution of joint operations and improving the quality of military advice provided to senior leaders—are so fundamental to the way DOD does business today that it is difficult to recall that it once conducted its operations quite differently.

DOD Challenges Prosecuting Joint Operations

Nearly 35 years ago, the Reagan Administration came into office largely convinced that the Pentagon was highly inefficient in its business and acquisition practices, and therefore established a Blue Ribbon Commission on Defense Management on July 15, 1985. The commission, which was headed by David Packard (founder of Hewlett-Packard and former Deputy Secretary of Defense), was instructed to “study defense management policies and procedures, including the budget process, the procurement system, legislative oversight, and the organizational and

(...continued)


7 Telephone interview with a former senior official, April 1, 2016.

8 See, for example, the spreadsheet on defense reform proposals collated and organized by the Center for Strategic and International Studies. The spreadsheet can be found at the following website (last accessed April 13, 2016). http://csis.org/images/stories/isp/160303_ISP_GN_Matrix.xlsx

operational arrangements, both formal and informal, among the Office of the Secretary of Defense, the Organization of the Joint Chiefs of Staff, the Unified and Specified Command system, the Military Departments, and the Congress.\(^\text{10}\) While the study explored many facets of the DOD and its management, the overall objective was to identify efficiencies and associated cost savings.

Yet several prominent shortcomings with the manner in which DOD conducted its military operations suggested to some observers that deeper organizational and structural challenges were plaguing the Department, and that these issues were not being sufficiently addressed by the Packard Commission. Congress therefore saw deep concerns develop as examples mounted that significant reforms to the Department of Defense were needed. Those examples included after action reviews of the following incidents: Desert One, Operations in Grenada, and the Marine barracks bombing in Beirut.

**Desert One, 1980**

After six months of planning, preparation, and training, in 1980 the U.S. military initiated a raid to rescue 53 American hostages being held in Tehran after the 1979 uprising in Iran. The operation failed. Only six of the eight helicopters arrived at Desert One, the rendezvous point in the middle of Iran, and a further helicopter suffered significant mechanical problems. Determining that the remaining helicopters did not have sufficient capacity to proceed, the mission was aborted. As the helicopters departed, one crashed into a C-130 aircraft carrying fuel and other servicemembers. All told, the United States lost eight military personnel, seven helicopters, and one C-130 aircraft, and left behind weapons, communications equipment, secret documents, and maps, all without making contact with the enemy.\(^\text{11}\)

After action reviews of the mission suggested that a key underlying problem with the mission was that the services were unable to operate together. As one observer wrote:

> [T]he participating units trained separately; they met for the first time in the desert in Iran, at Desert One. Even there, they did not establish command and control procedures or clear lines of authority. Colonel James Kyle, U.S. Air Force, who was the senior commander at Desert One, would recall that there were, “four commanders at the scene without visible identification, incompatible radios, and no agreed-upon plan.”\(^\text{12}\)

The inability of the services to operate together effectively led many to believe that the needs and interests of the individual military services were being prioritized over joint mission requirements. As the President’s National Security Advisor Zbigniew Brzezinski testified before the Senate Armed Services Committee:

> One basic lesson [to be learned from the failure of the mission] is that interservice interests dictated very much the character of the force that was used. Every service wished to be represented in this enterprise and that did not enhance cohesion and integration.\(^\text{13}\)


Grenada, 1983

Although Operation Urgent Fury (the 1983 U.S. military operation in Grenada to rescue U.S. medical students and other American Nationals after a Marxist coup) was generally viewed as a success, tactical and operational shortcomings marred the mission and became the subject of subsequent controversy. A primary issue was that units from the different U.S. military services conducting the mission proved unable to communicate with each other. Army elements could not use their equipment to communicate with sailors on the USS Guam to coordinate naval air support, and at times took drastic action to find ways to correct the problem. For example, some Army officers from the 82nd Airborne Division flew by helicopter to the USS Guam to begin coordinating air support, and even borrowed a Navy UHF radio to continue to do so while back in Grenada. Unfortunately, the Army officers operating the borrowed radio did not have the appropriate Navy clearance codes, rendering the equipment useless. It was also reported that one 82nd Airborne officer, frustrated with the situation, used an AT&T calling card from a civilian pay phone to call Fort Bragg and ask their higher headquarters to address the problem. Subsequent analysis led observers to conclude that the inability of the services to formulate and execute joint equipment and communications requirements was at the heart of the problem.

After action reviews also concluded that fire support from the Navy to the Army was a “serious problem,” and that the coordination between the two services ranged from “poor to nonexistent.” The two services did not coordinate their assault plans prior to the operation, and went into combat without any real sense of each other’s requirements, leading observers to conclude that the episode illustrated the “inadequate attention paid to the conduct of joint operations.” Another issue was the lack of sophisticated mapping capabilities. Troops had to use tourist maps. In conjunction with the aforementioned communications challenges, the lack of intelligence led to what some believed were unnecessary casualties. U.S. Navy Corsair airplanes accidentally attacked a mental hospital; two days later, they hit an a 82nd Airborne brigade headquarters building, wounding 17 U.S. soldiers. These issues, in conjunction with others including the lack of a designated ground commander and logistics issues, led a Senate study to conclude:

The operation in Grenada was a success, and organizational shortcomings should not detract from that success or from the bravery and ingenuity displayed by American servicemen.

However, serious problems resulted from organizational shortfalls which should be corrected. URGENT FURY demonstrated that there are major deficiencies in the ability of the Services to work jointly when deployed rapidly. The Services are aware of some of these problems and have created a number of units and procedures to coordinate communications. However, in Grenada, they either were not used or did not work. More fundamentally, one must ask why such coordinating mechanisms are necessary. Is it not possible to buy equipment that is compatible rather than having to improvise and concoct

---

14 Ibid., p. 365.
15 Ibid.
16 Ibid.
17 Ibid., p. 366.
20 Ibid., p. 59.
cumbersome bureaucracies so that the Services can talk to one another? Are the unified commands so lacking in unity that they cannot mount joint operations without elaborate coordinating mechanisms?

It further concluded:

The inability to work together has its roots in organizational shortcomings. The Services continue to operate as largely independent agencies, even at the level of the unified commands.\textsuperscript{21}

\textbf{Beirut, 1983}

Another major incident prompting congressional concern was the terrorist bombing of the Marine Barracks in Beirut, Lebanon, in October 1983, which killed 241 servicemen. Subsequent reviews of the tragic incident revealed significant shortcomings in the chain of command, which in the case of the Marine mission in Lebanon was described as "long, complex and clumsy."\textsuperscript{22} Analysis also revealed that the Unified Combatant Commander, in this instance, the Commander of United States European Command, had limited authority to direct service components within his area of responsibility to improve standards, especially when those components came from a different service. Despite the fact that U.S. European Command sought to improve the security for U.S. forces in Lebanon, its actual authority to do so was limited. General Smith, Deputy Commander of U.S. European Command at the time, said:

I really felt the Marines didn’t work directly for me. On paper, they were under our command, but in reality, they worked for the commander in chief, U.S. Naval Forces Europe, our naval component. They had their own operational and administrative command lines, which flowed from the naval component commander. I felt that antiterrorism training was primarily a navy and marine service issue. We didn’t have any control over that. We could advise, of course, but no more.\textsuperscript{23}

Prior to the enactment of the Goldwater-Nichols legislation, the services played a much larger role in the prosecution of military campaigns than they do today. The formal, \textit{de facto} operational chain of command led from the President, to the Secretary of Defense, to the Unified Combatant Commanders via the Joint Chiefs of Staff.\textsuperscript{24} The services were responsible for administrative functions. In practice, however, the situation was quite different. The services played a direct role in operations through their component commands (today, examples of service component commands include U.S. Army Pacific or U.S. Navy Europe).\textsuperscript{25} Each service had a component command within a Combatant Commander’s area of responsibility, and these service component commands often prioritized orders from their service’s headquarters in Washington over those of their Unified Combatant Commander.\textsuperscript{26} This dynamic was described by former Chairman of the Joint Chiefs of Staff Admiral Crowe:

\begin{itemize}
  \item \textsuperscript{21} Ibid.
  \item \textsuperscript{23} As quoted in Locher, \textit{Victory on the Potomac}, p. 158.
  \item \textsuperscript{24} At that time, the Joint Chiefs of Staff oversaw, but did not command, the Unified Commands. See David C Jones, "Why the Joint Chiefs of Staff Must Change," \textit{Presidential Studies Quarterly} (vol 12, no. 2, Spring 1982) p. 142.
  \item \textsuperscript{25} Locher, \textit{Victory on the Potomac}, p. 157
\end{itemize}
Like every other unified [combatant] commander, I could only operate through the Army, Navy, Air Force and Marine component commanders, who stood between me and the forces in the field.... Component commanders reported to their own service chiefs for administration, logistics and training matters, and the service chiefs could use this channel to outflank the unified commander. There was sizeable potential for confusion and conflict.  

This dynamic played out during U.S. operations in Lebanon:

Washington was bypassing EUCOM.... An investigation uncovered thirty-one units in Beirut that reported directly to the Pentagon. Orders to the carrier battle group off Lebanon came "straight from the jury-rigged 'Navy only' chain of command" that originated with the Chief of Naval Operations. Only after the Navy had set plans for fleet operations were superiors in the operational chain of command informed.  

Taken together, the Desert One, Grenada, and Marine Barracks bombing incidents suggested to Congress that deeper systemic and organizational issues were at work, preventing DOD from prosecuting joint operations successfully. In particular, issues with the operational chain of command, the quality of military advice given to civilian leaders, and the dominance of the services within the Department of Defense at the expense of joint requirements were all areas that Congress believed needed significant improvement.

The Goldwater-Nichols Legislation

Over time, many in Congress became convinced that the package of reforms identified by the Packard Commission—primarily focused on efficiency—were necessary, but not sufficient, to meet the challenges besetting the Pentagon at the time. Pointing to perceived operational shortcomings, some legislators, Administration officials, and military leaders became convinced that the organizational design of the Pentagon itself needed significant restructuring. The point was hammered home by then-Chairman of the Joint Chiefs of Staff David Jones, who testified:

It is not sufficient to just have resources, dollars and weapon systems; we must also have an organization which will allow us to develop the proper strategy, necessary planning, and the full warfighting capability.... We do not have an adequate organizational structure today.

The House and Senate Armed Services committees therefore decided to conduct their own independent reviews of the Pentagon’s structure, processes, and incentives, a process that lasted almost five years. Through this process, Congress drew the conclusion that the structure of the Department of Defense, as configured at that time, was organized primarily to serve the needs and priorities of the military services. While sensible in theory given the history of the U.S. Armed Forces, as a practical matter this encouraged inter-service rivalry that, in turn, led to operational failures.

The Joint Chiefs of Staff

Prior to the passage of the Goldwater-Nichols Act, the Joint Chiefs of Staff (JCS)—and the Joint Staff (JS) that supported it—were both very different organizations than they are today. Just prior to the passage of the Goldwater-Nichols Act, the Chairman of the Joint Chiefs of Staff and the service chiefs of the Army, Navy, Air Force, and Marine Corps were all statutory members. Their collective responsibility was to provide military advice to the Secretary of

27 Locher, Victory on the Potomac, p. 209.
28 Locher, Victory on the Potomac, Victory, p. 158.
29 Locher, p. 13
Defense, the National Security Council and the President. The Joint Chiefs of Staff was also tasked with supervising, but not commanding, the Combatant Commands, maintaining command and control networks with forces worldwide, and consulting with foreign militaries. The Joint Staff, which was dwarfed in size by the staffs of the services, supported the work of all four service chiefs and the Chairman. The structure was the result of a 1958 compromise between President Eisenhower, on the one hand, who sought to bring greater unity of command to Pentagon structures and, on the other, the military services, which sought to ensure that the needs and requirements of their individual departments were effectively represented during national security discussions.

By the 1980s, it became clear to some observers in the Pentagon and Congress that the system was not operating effectively and that the Joint Chiefs of Staff was rendering to national leaders what amounted to poor quality joint military advice. Former Secretary of State Dean Acheson is said to have quipped, "JCS papers reminded him of the little old lady who didn't know how she felt until she heard what she had to say." Reasons for this inadequate advice included the following:

- Dual-hatting. A number of observers noted that the responsibility of the service chiefs to advocate and advance their service interests was in direct conflict with their requirement to provide joint military advice as statutory members of the Joint Chiefs of Staff. More often than not, the interests of the military services were prioritized over those of the Joint Staff.
- Roles and Responsibilities. The collective JCS provided military advice to the President, the Secretary of Defense, and the National Security Council. This translated into a de facto veto by any service over any proposal or recommendation.
- A statutorily weak Chairman position. The Chairman was the only member of the Joint Chiefs of Staff that did not have his own deputy. He was also the only member of the JCS that did not have his own staff.
- A weak Joint Staff. The size of the Joint Staff was dwarfed by those of the services, and officers on the Joint Staff itself reported to all four service chiefs and the Chairman. The result was a cumbersome staffing process, with each service having the ability to veto initiatives or proposals at any time. Further, officers on the Joint Staff had little training or other preparation for operating in the joint environment.

The Goldwater-Nichols Act sought to address these structural deficiencies by making the Chairman, rather than the collective Joint Chiefs of Staff, the principal military advisor to the President, creating the position of Vice-Chairman of the Joint Chiefs of Staff, making the Joint Staff responsible to the Chairman of the Joint Chiefs of Staff, and creating career incentives for officers to acquire experience working in joint environments.


Contents of the Act

The Goldwater-Nichols Act sought to accomplish a number of objectives designed to improve the overall effectiveness of the Department. Still, the legislation's primary thrust was to improve the interoperability, or jointness among the military services at strategic and operational levels. Section 3 of P.L. 99-433 stated:

In enacting this Act, it is the intent of Congress, consistent with the congressional declaration of policy in section 2 of the National Security Act of 1947 (50 U.S.C. 401)—

(1) to reorganize the Department of Defense and strengthen civilian authority in the Department;

(2) to improve the military advice provided to the President, the National Security Council, and the Secretary of Defense;

(3) to place clear responsibility on the commanders of the unified and specified combatant commands for the accomplishment of missions assigned to those commands;

(4) to ensure that the authority of the commanders of the unified and specified combatant commands is fully commensurate with the responsibility of those commanders for the accomplishment of missions assigned to their commands;

(5) to increase attention to the formulation of strategy and to contingency planning;

(6) to provide for more efficient use of defense resources;

(7) to improve joint officer management policies; and

(8) otherwise to enhance the effectiveness of military operations and improve the management and administration of the Department of Defense.

It sought to accomplish these goals through a number of changes, including the following: 31

- Clarifying the military chain of command from operational commanders through the Secretary of Defense to the President;
- Giving service chiefs responsibility for training and equipping forces, while making clear that they were not in the chain of command for military operations;
- Elevating the Chairman of the Joint Chiefs of Staff relative to other service chiefs by making him/her the principal military advisor to the President, creating a Vice Chairman position, and specifying that the Joint Staff worked for the chairman;
- Requiring military personnel entering strategic leadership roles to have experience working with their counterparts from other services (so-called “joint” credit); 32 and

- Creating mechanisms for military services to collaborate when developing capability requirements and acquisition programs, and reducing redundant procurement programs through the establishment of the Office of the Under Secretary of Defense for Acquisition. 33

Despite Congress’s considerable deliberations, at the time consensus did not exist that significant DOD reforms were needed. Opposition to the Goldwater-Nichols Act was fierce in some quarters, in particular the Navy and Marine Corps; they believed that its implementation would severely degrade the ability of the services to wage the nation’s wars. 34 The legislation itself passed committee by one vote. 35

**Evaluations of the Goldwater-Nichols Legislation**

Five years later, the U.S. military successfully conducted Operation Desert Storm and other associated operations (such as Operation Provide Comfort). The clarification of the operational

---

31 P.L. 99-433
32 For more information on personnel reform and related issues, see CRS Report R44340, Goldwater-Nichols and the Evolution of Officer Joint Professional Military Education (JPME), by Kristy N. Kamarck.
33 The change was reflected in 10 U.S.C. §133. In 1993, “and Technology” was added; in 1999 the office was re-designated “Acquisition, Technology & Logistics.”
chain of command, as well as the advances in jointness that were made as a result of the Goldwater-Nichols legislation, were viewed by many as instrumental to that success. Then-Chairman of the Joint Chiefs of Staff Colin Powell testified that, "You will notice in Desert Storm nobody is accusing us of logrolling and service parochialism and the Army fighting the Air Force and the Navy fighting the Marine Corps. We are now a team. The Goldwater-Nichols legislation helped that." Indeed, as Admiral Leighton Smith wrote about the mission to provide humanitarian relief to the Kurds in Northern Iraq (Operation Provide Comfort):

The good news about this operation was that from a command relationship perspective, Jim Jamerson, and later our Chairman, General Shalikashvili, knew exactly for whom they worked and to whom they reported. That joint task force, like the five others we put together during my 21 months in the J-3 [Joint Staff Operations] job, all reported directly to the CINC, bypassing the component commanders ... and the inevitable service guidance that existed in the Pentagon in the pre-Goldwater-Nichols days ... there was none of the direct calls from Washington to the commander in Turkey or the individual service component commanders, to give operational guidance or demand information that should rightfully go through the unified commander."

Still, some observers maintain that the act has produced unintended consequences that ought to be mitigated. Namely, some contend that Goldwater-Nichols may have gone too far in prioritizing joint over individual service requirements and that a better balance must be struck. Specifically, one of the most commonly voiced criticisms pertains to the act's provisions for joint personnel management, and whether the joint officer requirements lead to the development of officers with an appropriate mix of service and joint experiences. Others maintained (and still do) that the act did little to address perceived inefficiencies in defense spending. It also failed to curtail the growth of staffing in the Office of the Secretary of Defense and the Defense Agencies. Finally, while many believe that the quality of military advice provided to the Secretary of Defense and the President has improved as a result of the act's strengthening of the Chairman of the Joint Chiefs of Staff position, some contend the Department still has room for improvement when developing its strategies and plans.

Another school of thought maintains that the act introduced changes that were necessary, but not sufficient, to meet the challenges of the post-Cold War environment, and that further reform of

38 Leighton W. Smith, p. 29.
41 Arnold Punaro, Statement before the Senate Armed Services Committee: The Urgent Need to Reform and Reduce DOD's Overhead and Infrastructure, November 17, 2015.
42 Locher, Did It Work? p. 111.
the national security architecture was needed. In particular, the experience of post-Cold War contingency and stability operations demonstrated the benefit of adequately trained and resourced interagency partners (for example, State, USAID, Treasury, and so on). Ten years after the initial passage of the Goldwater-Nichols Act, then-Chairman of the Joint Chiefs of Staff Shalikashvili observed:

A strong, well-understood link among the Departments of Defense, State, Justice, Commerce and the entire interagency community will be vital. Look at many of the most recent challenges to U.S. national interests around the world: Rwanda and Zaire, Bosnia, Haiti, the Arabian Gulf. In every one of these operations, success required the involvement of a wide variety of interagency participants.

On balance, the Goldwater-Nichols Act has generally been lauded as a major breakthrough in effective defense management, but there are differences of opinion on the ultimate outcome of the Goldwater-Nichols legislation. Some contend that the act may have produced unintended consequences and unnecessarily diminished the services; in the view of others, there are areas in which the reform agenda did not go far enough. As described in the next section, some of these views are being carried forward into the current debate on defense reform.

The Strategic Context in 2016

Thirty years later, the strategic environment has shifted dramatically. Since the enactment of the Goldwater-Nichols legislation, a number of important historical events have taken place, starting with the end of the Cold War. Subsequently, the United States performed crisis management and contingency operations globally, in theaters including Iraq, the Balkans, Somalia, and Colombia. After the September 11, 2001, terror attacks, the United States undertook major counterinsurgency campaigns in Iraq and Afghanistan, as well as a number of smaller operations as part of its “global war on terror.”

Emerging Threats

The international security environment was already demanding when the Goldwater-Nichols legislation was enacted, yet most observers agree it has become significantly more complex and unpredictable in recent years. This is challenging the United States to respond to an increasingly diverse set of requirements. As evidence, observers point to a number of recent events, including (but not limited to)

- the rise of the Islamic State, including its military successes in northern Iraq and Syria;
- the strength of drug cartels in South and Central America;

43 Cole, p. 64.
• Russian-backed proxy warfare in Ukraine;
• heightened North Korean aggression;
• Chinese “island building” in the South China Sea;
• terror attacks in Europe;
• the ongoing civil war in Syria and its attendant refugee crisis; and
• the Ebola outbreak in 2014.

Indeed, as Secretary of Defense Ashton Carter remarked before the House Armed Services Committee in March 2016:

Today’s security environment is dramatically different—and more diverse and complex in the scope of its challenges—than the one we’ve been engaged with for the last 25 years, and it requires new ways of thinking and new ways of acting.47

What makes today’s issues uniquely problematic—perhaps even unprecedented—is the speed with which each of them has developed, the scale of their impact on U.S. interests and those of our allies, and the fact that many of these challenges have taken place—and have demanded responses—nearly simultaneously.48 Further complicating matters, U.S. adversaries appear to be using tactics and operations that are provocative, but which tend to fall short of necessitating a large-scale military response. Adapting U.S. military and civilian defense institutions to operate effectively in these “grey zone” conflict spaces, wherein adversaries are not immediately obvious, and interests are advanced using a combination of military and nonmilitary tactics, is becoming an increasingly important priority for DOD leaders.49 Altogether, these dynamics have created the extremely high degree of complexity with which the United States must grapple, placing increasing demands on the U.S. national security architecture generally, and the Department of Defense in particular.

The Fiscal Challenge

These changes in the international security landscape are occurring against a backdrop of U.S. defense “austerity,” a common shorthand term for fiscal restrictions on the DOD budget. According to some observers as early as 2010:

The aging of the inventories and equipment used by the services, the decline in the size of the Navy, escalating personnel entitlements, overhead and procurement costs, and the growing stress on the force means that a train wreck is coming in the areas of personnel, acquisition and force structure.50

Background: The Federal Deficit and the Budget Control Act

The Budget Control Act of 2011 was enacted in response to congressional concern about rapid growth in the federal debt and deficit. The federal budget has been in deficit (spending exceeding revenue) since FY2002, and incurred particularly large deficits from FY2009 to FY2013. Increases in spending on defense, lower tax receipts, and responses to the recent economic downturn all contributed to deficit increases in that time period. In FY2010, spending reached its highest level as a share of GDP since FY1946, while revenues reached their lowest level as a share of GDP since FY1950.

The BCA placed statutory caps on most discretionary spending from FY2012 through FY2021. The caps essentially limit the amount of spending through the annual appropriations process for that time period, with adjustments permitted for certain purposes. The limits could be adjusted to accommodate (1) changes in concepts and definitions; (2) appropriations designated as emergency requirements; (3) appropriations for Overseas Contingency Operations/Global War on Terrorism (OCOR, e.g., for military activities in Afghanistan); (4) appropriations for continuing disability reviews and redeterminations; (5) appropriations for controlling health care fraud and abuse; and (6) appropriations for disaster relief.

Source: CRS Report R42506, The Budget Control Act of 2011 as Amended: Budgetary Effects, by Grant A. Driessen and Marc Labonte

Yet some have argued that the Budget Control Act of 2011 (and subsequent amendments) placed significant constraints on the Department’s ability to address these challenges, allocate monies toward critical priorities, and effectively divest from obsolete facilities and equipment programs.\(^3\) As the 2014 Quadrennial Defense Review Panel asserted:

> the defense budget cuts mandated by the Budget Control Act of 2011, coupled with the additional cuts and constraints on defense management under the law’s sequestration provision ... have created significant investment shortfalls in military readiness and both present and future capabilities. Unless reversed, these shortfalls will lead to greater risk to our forces, posture and security in the near future.\(^4\)

The impact of financial reductions imposed by the Budget Control Act, along with the way DOD resources are allocated, has led many observers to conclude that there has been a significant, deleterious impact on the readiness and capability of the force.\(^5\) Yet the United States now spends over $600 billion per year on activities associated with the DOD (including the base budget and Overseas Contingency Operations account)\(^6\) which is, according to some estimates, comparable to the total spent by the next eight largest defense spending countries combined.\(^7\) This often perceived mismatch between inputs and outputs appears to be one key strategic-level impetus for the reform of DOD’s acquisition systems. According to H.Rept. 114-102:

---

\(^3\) It should be noted that another view on the BCA was that the Department had sufficient flexibility to absorb the constraints imposed by BCA spending caps. See The New York Times Editorial Board, “Defense and the Sequester,” The New York Times, February 24, 2013. http://www.nytimes.com/2013/02/25/opinion/defense-and-the-sequester.html. Still, most observers maintain that unpredictable funding levels and budget caps have negatively impacted the force.


The committee believes that reform of the Department of Defense is necessary to increase the effectiveness and efficiency of the defense enterprise to get more defense for the dollar. This is necessary to improve the military’s agility and the speed at which it can adapt and respond to the unprecedented technological challenges faced by the nation.56

In summary, compared to the strategic context 30 years ago, the current international security environment is generally characterized by increased, and more dynamic, security challenges. Despite the considerable size of the DOD budget, fiscal constraints have forced the Department to make tough choices on priorities, and have significantly affected force readiness, among other things. In short, some scholars have found that requirements are going up while resources are plateauing, at best.57 This is leading many observers to wonder whether necessary programmatic “belt tightening” will sufficiently enable the Department of Defense to effectively meet today’s and tomorrow’s threats.

Why Reform DOD Today?

It is within this context that Congress has undertaken its review of the Goldwater-Nichols legislation, as well as a broader review of DOD’s organization and structure. Observers in this process seem to approach the problem differently, based upon their own experiences with, or within, the Department of Defense.58 Some maintain that Goldwater-Nichols led to the positioning of the United States military as the “finest fighting force” in the world, and therefore question whether major DOD reforms are needed.59 Yet there are several fundamental, first order questions that seem to be driving the current examination of DOD’s structure. These include, but are not limited to the following:

- Why, after the expenditure of nearly $1.6 trillion and over 15 years at war in Iraq and Afghanistan, has the United States had such perceived difficulty translating tactical and operational victories into sustainable political outcomes?60

- Why, despite the expenditure of now over $600 billion per year on defense, is the readiness of the force approaching critically low levels, according to senior military officials, while the number of platforms and capabilities being produced are generally short of perceived requirements?61

---

57 Andrew Krepinevich, Statement before the Senate Armed Services Committee on Defense Strategy, October 28, 2015, p. 12.
58 See, for example, the CSIS spreadsheet which organizes DOD reform proposals presented in SASC testimony into nine categories. See also: Frank Hoffman and Michael Noonan, “Defense Reform Redux,” E-Notes, Foreign Policy Research Institute, February 2016, http://www.fpri.org/article/2016/02/defense-reform-redux/
• Why, despite tactical and operational level adaptations around the world, is DOD often seen as having difficulty formulating strategies and policies in sufficient time to adapt to and meet the increasingly dynamic threat environment of the 21st century?62

• What challenges, in either structure or process (or both), might lead to perceived DOD difficulties in executing current military operations while simultaneously planning for and obtaining resources for future capabilities?

No single answer exists for these questions. No one decision, no one individual, no one process led to these arguably less than desirable outcomes. Taken together, however, the issues raised by these questions suggest the systemic nature of the challenges with which the Department of Defense appears to be grappling. In other words, they suggest that DOD’s organizational architecture and culture may merit serious review and analysis.

A Secretary at War

In his memoirs, former Secretary of Defense Robert Gates expresses considerable frustration with the manner in which the Pentagon prosecuted wars. “Even though the nation was waging two wars, neither of which we were winning, life at the Pentagon was largely business as usual.”63 He goes on to identify a number of structural issues he experienced with DOD, including the following:

• The absence of a senior DOD official whose specific job is to ensure commanders and troops in the field have what they need;

• The size and structure of the Pentagon’s bureaucracy, which requires a large number of organizations be involved in “even the smallest decisions,” leading to paralysis when it came to decision-taking;

• The large number of “filters” between the field commanders and the Secretary of Defense, which could delay or altogether halt the acquisition of urgently required equipment or other capabilities;

• The necessity to work outside of the Pentagon’s formal staffing structures to accomplish key tasks, such as fielding Mine Resistant Ambush Protected (MRAP) Vehicles;

• The services’ view that complex counterinsurgency operations were an aberration, and their subsequent prioritization of training and equipping of troops to fight future conflicts for which they had natural comparative advantage, such as conventional force-on-force battles, instead of adapting to the counterinsurgency fight.

Noting DOD’s overall lack of agility, Gates finally concludes that “[t]he Department of Defense is structured to plan and prepare for war, but not to fight one.”


The Defense Management and Reform Challenge

DOD’s mission is to “provide the military forces needed to deter war and protect the security of our country.”64 In order to do so, DOD must plan for current and future threats and then prepare military forces with the training and other military capabilities necessary to meet those threats. It must also propose and manage a budget appropriate to the nation’s defense needs and articulate

(...continued)

Committee on Readiness on U.S. Marine Corps Readiness,” March 15, 2016, p. 7.
acceptable levels and areas of risk. While simple in theory, orchestrating and synchronizing these activities is a highly complex endeavor.

Hundreds of studies, comprising thousands of recommendations and tens of thousands of pages, have been dedicated to reforming the Department of Defense and its many facets. The scale and complexity of the DOD make it a uniquely challenging organization to manage. As one management expert stated in 1997:

> The most difficult problem in the entire world right now is the transformation of Russia into a democratic, free-market economy. You may not realize that the second most difficult problem I can possibly envision is that of reforming the Defense Department.\(^5\)

Over the duration of the Department’s history, a number of Administrations have sought to improve its management and efficiency. These reforms have generally taken one of three approaches. The first advocates for more centralization, shifting more authority and resources from the military departments to joint institutions and/or Office of the Secretary of Defense (OSD) control in order to improve interoperability and efficiency. The second approach favors more decentralization, through retaining or bolstering semi-autonomous military services, properly guided by OSD decisionmaking and resource allocation processes, thereby promoting creativity and innovation through competition. The third “business matrix” approach attempts to infuse business management structures into existing Pentagon architectures using cross-functional teams, boards, and councils to promote collaboration.

Yet, as noted by the U.S. Commission on National Security in the 21\(^{st}\) Century (the Hart-Rudman Commission):

> The current structure of DOD’s major staffs (and their functions) represents a meshwork of all three models, and the net result has been a diffusion of authority, responsibility and accountability. In many cases, the three different paradigms work at cross-purposes to obstruct and block each other. This dilutes the Department’s ability to transform itself internally. It hinders the identification of problems, the development of alternative solutions, and the elevation of decisions to senior officials for resolution.\(^6\)

**Conceptualizing DOD’s Enterprise-Level Functions**

The diagram below depicts one way to think about managing the defense enterprise (see Figure 1). On behalf of the President, the Secretary of Defense must oversee and balance three distinct but highly interrelated functions that support all of DOD’s activities: requirements, capabilities, and costs. These broad functions can usefully be conceptualized as three points of a triangle.

- The first, *requirements*, refers to the Department’s work to analyze the current and future threat environment, define the missions and tasks that different DOD components must be prepared to accomplish, and organize itself in order to do so (i.e., through the Unified Command Plan).\(^7\)

---


\(^6\) Ibid., pp. 12-13

\(^7\) CRS Report R42077, The *Unified Command Plan and Combatant Commands: Background and Issues for Congress*, by Andrew Feickert.
• DOD must then define, develop, and manage the military capabilities—in terms of equipment, training, and posture—necessary to accomplish those missions and tasks.

• Finally, DOD must manage its costs in a manner that accounts for current and future expenditures on its worldwide operations, as well as the personnel, facilities, and processes comprising the defense institution itself.

In each of these “points,” the Department must identify, and to the extent possible mitigate, any risks associated with under- or over-prioritizing any particular activity or program.

**Figure 1. DOD Enterprise-Level Management**

Three Core Activities

Managing a government organization the size of the Department of Defense—with over 3 million civilian and military employees (of which 450,000 are overseas) and several hundred thousand individual buildings and structures located at more than 5,000 different locations—cannot, nor will it ever, be straightforward. This, in turn, makes managing and balancing the “points” of the triangle comprising DOD’s activities extremely difficult.

Each point of the triangle in Figure 1 represents the actions and programs of hundreds of different organizations and units, at multiple echelons at the strategic, operational, and tactical levels. The enormity of the DOD management challenge is exacerbated by the Department’s internal complexity and the wide variety of external stakeholders in DOD’s operations and activities (including Congress, industry, allies, and partners). As such, in many ways the challenge of DOD reform presents the characteristics of a “wicked” problem, commonly thought of as a social or cultural problem that is difficult or impossible to solve, and one in which solving one aspect of the problem often leads to new, equally formidable challenges. If past trends hold, reforming one aspect of the Department will almost inevitably have unintended consequences that will create new problems, likely necessitating further reform.

**Efficiency vs. Effectiveness**

Efficiency and effectiveness are often conflated in the defense reform debate. This is because a number of scholars and practitioners maintain that reforming the Department of Defense in order to improve its overall efficiency—defined as the “ability to do something or produce something without wasting materials, time, or energy”—will also improve DOD’s effectiveness, or its

---

68 Ibid.

ability to accomplish its assigned tasks.70 As the logic goes, taking actions such as constraining the resources associated with DOD’s bureaucracy and headquarters, or requiring the services to procure equipment in conjunction with each other, forces the Department to better prioritize its activities and allocate its resources. Yet while effectiveness and efficiency can be interrelated objectives, it is important to note that they are not the same thing. In fact, if not carefully managed, the two goals can actually work at cross-purposes with each other when pursued simultaneously.

Within the Department of Defense, the reduction and subsequent increase in the acquisition workforce may provide an example of efficiency coming at the expense of effectiveness. According to the Government Accountability Office:

The acquisition workforce of the Department of Defense (DOD) must be able to effectively award and administer contracts totaling more than $300 billion annually. The contracts may be for major weapons systems, support for military bases, consulting services, and commercial items, among others. A skilled acquisition workforce is vital to maintaining military readiness, increasing the department’s buying power, and achieving substantial long-term savings through systems engineering and contracting activities.71

Concerns during the 1980s that the acquisition workforce (AW) was under-skilled and over-manned prompted the Department to reduce the number of personnel associated with the AW in the 1990s. As part of Defense budget reductions and efficiency improvements, the civilian and military acquisition workforce was reduced by 14%, and the Department began relying on contractors to perform a variety of acquisition-related functions.72 DOD also lost workers with critical acquisition skill sets.73 Subsequently, experts found that the AW was ill-prepared or suited to manage the complex and urgent contracting requirements associated with expeditionary operations in Iraq and Afghanistan.74 The Section 1423 report also noted, “[i]n general, the demands placed on the acquisition workforce have outstripped its capacity.”75 Efforts to reconstitute the acquisition workforce in order to make it more effective began in earnest in 2009.76

Headquarters Reductions

Reducing the size of various headquarters has been a consistent theme of defense reformers for decades. Indeed, participants in the Goldwater-Nichols debates over 30 years ago saw the growth in Pentagon and headquarters bureaucracy as a key challenge to DOD efficiency and effectiveness. Today, the preponderance of defense scholars and experts maintain that reducing

70 http://www.merriam-webster.com/dictionary/efficiency
72 Ibid.
DOD bureaucracy and headquarters staffs is necessary in order to improve the Department’s decisionmaking and agility while simultaneously controlling costs. In their view, doing so will force components across the Department to prioritize their activities and divest themselves of unnecessary functions. This rationale has, in part, led DOD to reduce its headquarters staff by 25% and Congress to restrict the amount of funding available to DOD for headquarters, administrative, and support activities.

Implementing these reductions, however, is proving problematic. Many of the roles and missions performed by different offices around the Department have been mandated by senior leaders or Congress; staff reductions mean that the same workload is being shouldered by fewer people, leading in some instances to overworked staffs. Unless the Department finds ways to divest itself of certain functions or tasks, headquarters reductions could compromise DOD’s effectiveness. As one observer describes this dynamic:

[...] any reduction in staff will save a commensurate amount of resources, but it will not—without needed reforms—generate greater effectiveness. Just cutting staff ignores real problems, like our inability to collaborate across organizational lines on multifunctional problems.

Efforts to improve fiscal efficiency without balancing the ramifications for overall mission effectiveness can create significant challenges for the Department. A number of observers maintain that the Department of Defense is a bloated organization, with too many staffs at higher headquarters. Yet the fact remains that most offices or agencies are responsible for a task or mission that was, at least at one point (if not at present), deemed critical. For example, one reason the Joint Staff is now 4,000 persons—considered by many to be too large—is due to the fact that during the disestablishment of Joint Forces Command, essential joint service functions were transferred to the Joint Staff. Unless or until Congress or DOD leadership deems those functions no longer indispensable, cutting staffs to improve efficiency may result in degraded mission effectiveness.

---

79 Interviews with current Pentagon employees, March 2016.
### The Challenge of Organization Design

In some ways, the design of an organization can be likened to the plumbing of a house: unseen, yet essential to its functioning. Much like plumbing, when the design of an organization proves unable to enable its intended functions, the consequences can be ugly. As an example, some maintain that one of the critical reasons that Kodak has deteriorated to such a significant degree was because it could not adapt its organization to better comprehend, and then respond to, changing market circumstances. As one management scholar writes, “[p]oor organizational design and structure results in a bewildering morass of contradictions; confusion within roles, a lack of coordination among functions, failure to share ideas, and slow decision-making, bring[ing] managers unnecessary complexity, stress and conflict.”

Optimizing an organization’s design is a challenge that is not unique to the Department of Defense. Every organization—be it a business or public sector agency—must organize its people, processes, and structures in a manner that enables the group as a whole to achieve its objectives. Accordingly, there is no one “right” answer to organization design; rather, an organization is effectively structured when it helps its leaders define their strategy and enables that strategy to be predictably executed. This is why many large companies routinely revisit their organizational structures in order to remain competitive in the marketplace.

Organization design theory offers an analytic lens through which observers can evaluate whether DOD is effectively structured to meet current and future objectives. Different management consultants utilize a variety of different models when testing whether an organization’s structures enable the group to accomplish its objectives. In so doing, some of the key questions they ask include:

<table>
<thead>
<tr>
<th>Design Question</th>
<th>...Applied to DOD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The “First Principles” Test.</strong> What is the business’s value proposition and its sources of competitive advantage?</td>
<td></td>
</tr>
<tr>
<td><strong>Rationale:</strong> A clear statement of what a business is good at, relative to other competitors, illuminates the core activities around which an organization ought to be designed.</td>
<td></td>
</tr>
<tr>
<td><strong>What are DOD’s unique advantages in the advancement of national security, relative to other agencies and departments?</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Challenge:</strong> The international security environment in which DOD must operate has arguably led the Department to take on roles and missions, such as post-conflict stabilization, that some observers believe it is not ideally suited toward.</td>
<td></td>
</tr>
</tbody>
</table>

| **The Market Advantage Test.** Which organizational activities directly deliver on that value proposition—and by contrast, which activities can the company afford to perform in a way equivalent to its competition? Does the design direct sufficient management attention to the sources of competitive advantage in each market?  |
| **Rationale:** Those activities that are crucial to delivering on a value proposition should be prioritized and resourced above other functions. |
| **What are the activities DOD engages in that enable it to make its unique contribution to national security? What are the functions or areas in which the Department must build and maintain excellence? Are there functions or tasks that are better suited to other USG agencies?** |
| **Challenge:** the blurring of lines between peacetime and conflict, as well as DOD’s assumption of many tasks that have historically been accomplished elsewhere in the executive branch, has made it difficult to establish what tasks must be accomplished to advance U.S. interests, and whether the Department of Defense ought to be |

---


The People Test. Does the design reflect the strengths, weaknesses, and motivations of its people? What kind of leadership and culture are needed to achieve the value proposition? Which organizational practices are required to reinforce organizational intent?

Rationale: Cultural values are woven into the way people behave in the workplace. Without addressing leadership and culture, employees often adhere to old practices and work around, instead of working with, a new system.

The Redundant-Hierarchy Test. Does the design of the organization have too many levels? What, specifically, does each level of the organization add to the accomplishment of core tasks? How do “parent” units enable subordinate teams to accomplish key missions?

Rationale: Too much hierarchy within an organization can impede agile decisionmaking and stifle innovation (seven or eight layers between an employee and CEO is generally believed to be the maximum supportable number of layers). Those levels within an organization that cannot demonstrate their value added could be candidates for elimination.

What levels might DOD usefully eliminate in order to improve agility and encourage innovation?

Challenge: In part due the fact that DOD has taken on so many roles and missions, DOD is now an organization that is simultaneously highly vertical (with many layers of management) and highly horizontal (with many offices “clearing” on any given memorandum). This is leading to what Former Under Secretary for Policy Michele Flournoy describes as the “tyranny of consensus,” and poor-quality civilian and military advice.

Drawing analogies between DOD and the private sector has clear limitations. Unlike businesses, the Department of Defense is not organized to deliver profits to its stakeholders. Further, the consequences of risks taken are measured in casualties; while failing corporations go bankrupt, DOD failure can result in national failure. Still, these design questions can help observers understand whether the organizational architecture of the Department of Defense is optimized—or not—to enable its personnel to meet current and emerging national security challenges.

Framing the Problem: Current DOD Reform Concepts

While consensus on specific reform solutions remains elusive, many scholars and practitioners agree on the characteristics that DOD must have if it is to grapple effectively with current and emerging strategic challenges. Namely, many believe that the Department must be better able to respond to multiple complex contingencies around the world, both anticipated and unforeseen. Rapid adaptation and “agility” is therefore necessary. With respect to the latter point, as noted by Chairman of the House Armed Services Committee Mac Thornberry in January 2016:

86 Jones, p. 125.
I think there are two primary characteristics that describe the military capability that we need. And they are strength and agility. We know from sports that you can't do with one and not the other. You have to have both.99

In March 2016, Senate Armed Services Committee Chairman John McCain fleshed out his own concept of what DOD must be able to do:

I believe we have a rather clear definition of the challenge that we all must address. The focus of Goldwater-Nichols was operational effectiveness, improving our military's ability to fight as a joint force. The challenge today is strategic integration. By that, I mean improving the ability of the Department of Defense to develop strategies and integrate military power globally to confront a series of threats, both states and non-state actors, all of which span multiple regions of the world and numerous military functions.99

The Center for Strategic and International Studies (CSIS) "Open Letter on Defense Reform," signed by a bipartisan group of senior defense observers and practitioners, frames the DOD reform challenge slightly differently. Instead of articulating the desired characteristics of a future DOD, they focus on some of the key organizational problems that, in their view need to be overcome:

the Defense Department, and even more so the broader U.S. national security complex, appear[s] sclerotic in their planning, prioritization, and decision-making processes. We should identify better ways to pace and get ahead of this changing environment.

Second, the defense enterprise is too inefficient. These two problems are intertwined. There appears to be significant duplication of responsibilities and layering of structure, which contributes materially to the perception that we are at risk of being outpaced and outwitted by adversaries. Moreover, our military and defense civilian personnel systems, requirements and acquisition systems, security cooperation and foreign military sales systems, and strategy, planning, programming, and budgeting systems reflect twentieth-century approaches that often seem out of step with modern best practices.91

While experts convened by CSIS could not agree on specific reform proposals, they did note that two principles should guide defense reform efforts:

First, we must sustain civilian control of the military through the secretary of defense and the president of the United States and with the oversight of Congress.

Second, military advice should be independent of politics and provided in the truest ethos of the profession of arms.92

On April 5, 2016, Secretary of Defense Ashton Carter articulated his ideas regarding defense reform and the areas within the Department that need improvement:

It's time that we consider practical updates to this critical organizational framework, while still preserving its spirit and intent. For example, we can see in some areas how the pendulum between service equities and jointness may have swung too far, as in not involving the service chiefs enough in acquisition decision-making and accountability; or where subsequent world events suggest nudging the pendulum further, as in taking more steps to strengthen the capability of the Chairman and the Joint Chiefs to support force

---

99 Chairman Mac Thornberry, Speech to the National Press Club, January 16, 2016.
90 Remarks by Senator John McCain, Senate Armed Services Committee Holds Hearing on the Defense Department Budget Posture, Congressional Quarterly, March 1, 2016
92 Ibid.
management, planning, and execution across the combatant commands, particularly in the face of threats that cut across regional and functional combatant command areas of responsibility, as many increasingly do.\footnote{U.S. Department of Defense, \textit{Remarks by the Secretary of Defense on "Goldwater-Nichols at 30: An Agenda for Updating"}, Washington DC, Center for Strategic and International Studies, April 5, 2016. \url{http://www.defense.gov/News/Speeches/Speech-View/Article/713736/remarks-on-goldwater-nichols-at-30-an-agenda-for-updating-center-for-strategic}}

Secretary Carter further intimated that DOD will be augmenting some of its internal processes as well as submitting statutory changes to Congress for consideration.
Lessons Encountered from the Long War

Seeking to enable the Department of Defense to better prepare itself for future conflicts, the National Defense University conducted a study of the strengths and weaknesses of the U.S. approach to its post September 11th campaigns. Some of the key outcomes from that study include the following:

**Civilian-military relations.** The study identified significant strategic-level disconnects between the military staffs and the civilian leadership they supported in both the Bush and Obama Administrations. As conditions on the ground in Iraq deteriorated in 2006, President Bush decided to go against the recommendations of his military and defense leadership, and instead authorized a "Surge" of forces that was advocated by external advisors. After a series of unfortunate media missteps by several senior military leaders under the Obama Administration, a "perception formed in the minds of senior White House staff that the military had failed to bring forward realistic and feasible options, limiting serious consideration to only one, and that it had attempted to influence the outcome by trying the case in the media, circumventing the normal policy process" (p. 412). In summary, "[t]he military did not give President Bush a range of options for Iraq in 2006 until he insisted on their development, nor did they give President Obama a range of options for Afghanistan in 2009." (p. 143).

**Strategy Formulation and Adaptation.** A gap in overall national strategy formulation and evaluation was identified by the authors. In the first instance, the authors maintain that the United States failed to fully appreciate the strategic context in which it was operating, as well as the on-the-ground political and military realities in Iraq and Afghanistan. With respect to Iraq, the study also points out that the lack of mechanisms for strategic-level reevaluation and adaptation prevented needed reassessment—and readjustment—until it was clear that the United States was on the verge of failing (p. 143).

**National-level decisionmaking.** Noting that "both civilian and military leaders are required to cooperate to make effective strategy, yet their cultures vary widely," the authors maintain that "[c]ivilian national security decision-makers need a better understanding of the complexity of military strategy and the military's need for planning guidance." The authors go on to note that "strategy often flounders on poorly defined or overly broad objectives that are not closely tied to available means" (p. 413). In their view, military leaders must improve their ability to work with their civilian counterparts in strategy formulation.

**Unity of Effort.** "Whole-of-government efforts are essential in irregular conflicts... The United States was often unable to knit its vast interagency capabilities together for best effect." Furthermore, "Policy discussions too often focused on the familiar military component (force levels, deployment timelines and so forth) and too little on the larger challenge of state-building and host-nation capacity" (p. 145).

**Strategic Communications.** "Making friends, allies, and locals understand our intent has proved difficult... our disabilities in this area—partly caused by too much bureaucracy and too little empathy—stand in contradistinction to the ability of clever enemies to package their message and beat us at a game that was perfected in Hollywood and on Madison Avenue" (p. 15).

DOD guidance has specified that the United States will no longer plan to conduct large-scale counterinsurgency or stability operations. Still, some observers maintain that these challenges, if left unresolved, will hamper DOD's efforts to wage any future military campaigns, and particularly those that require U.S. military forces to operate in "grey zone" conflicts.


Current Defense Reform Proposals

As noted earlier in this report, no consensus currently exists regarding specific recommendations to "fix" the Pentagon. This, in part, stems from a lack of agreement on the nature of the bureaucratic challenges currently besetting the Department of Defense and preventing it from accomplishing what many perceive to be core tasks.

During hearings held in the second session of the 114th Congress, experts recommended scores of proposals to reform DOD. These are in addition to the many other proposals advocated by a variety of scholars and practitioners across the defense and national security policy community. For purposes of bringing a degree of analytic coherence and clarity to the present discussion, CRS grouped together and condensed similar DOD reform proposals raised by experts in their testimonies to the Senate Armed Services Committee. Reform suggestions tabled outside the
context of the hearings were not included. CRS then sought to better link each set of recommendations with the problems they are attempting to solve through organizing the proposals into one of four categories. Three of these categories align with the core areas of defense enterprise management articulated earlier in this report: managing costs, formulating requirements and building capabilities. The fourth category includes proposals for reforming the broader interagency national security system. This listing of defense reform proposals should be treated as illustrative of the state of the debate at present; evaluating the relative strengths and weaknesses of each set of proposals is beyond the scope of this report.

External Defense Expert Reform Proposals

During the second session of the 114th Congress, the Senate Armed Services Committee held a series of hearings to discuss areas ripe for reform within the Department of Defense. Through the duration of the proceedings, various national security experts proposed over 160 different recommendations for reforming the Pentagon. What follows below is an illustrative sample, rather than an exhaustive listing, of the many proposals suggested by experts.

Formulating Requirements

There is widespread belief among observers that the processes the Department uses to formulate its strategies and strategic requirements in order to grapple with current and emerging security challenges are “broken.” Still, there is very little agreement on what ought to be done to address this. This category of recommendations pertains to problems identified with the way in which the Department prepares its strategies, particularly global strategies, and organizes itself to execute its policies. Proposals for possible reform include the following.

- Improving DOD strategy-making by:
  - Generating better strategy documents. Proposals included replacing the Quadrennial Defense Review (now the Defense Strategy Review) with a classified internal defense strategy, and creating a comprehensive strategy review akin to President Eisenhower’s Project Solarium.
  - Reforming the central institutions for strategy formulation. Proposals included creating an Operations versus Plans division of labor within the Office of the Secretary of Defense (akin to the J3/J5); institutionalizing “red teaming” of strategies; building a competitive process for alternative future force planning, run by the Deputy Secretary of Defense; and creating a Joint General Staff exclusively focused on strategy formulation (more on this recommendation below).

- Improving the way DOD organizes itself to accomplish strategic objectives and execute operations by:
  - Augmenting the Unified Command Plan. Proposals vary, but included the elevation of United States Cyber Command to a four-star Unified Combatant

---

94 Flournoy, p. 3
96 Project Solarium was a national strategy-making exercise convened by President Eisenhower in order to build consensus on how to deal with the Soviet Union and its expansionism.
Command (COCOM), the collapse of U.S. European Command and U.S. Africa Command into one COCOM, and the collapse of U.S. Northern Command and U.S. Southern Command into another single COCOM. Others recommended against merging the regional combatant commands. Another recommendation was to revisit altogether the regions of responsibility for geographic Combatant Commands.

- **Augmenting existing command structures.** Proposals vary, and are in some ways in opposition. These included placing the Chairman of the Joint Chiefs of Staff in the operational chain of command; giving Service Secretaries more authority for military operations and operational planning; retaining the current “J-code” staff structures of the Joint Staff; and disestablishing service component commands and instead replacing them with Joint Task Forces. It should be noted that the proposal to grant greater operational responsibility to the Service Secretaries (promoting decentralization) is in some ways the opposite recommendation to putting the CJCS in the operational chain of command (promoting jointness). Others recommended against any proposal that diminishes the authority of the Secretary of Defense to make key decisions, including placing the CJCS (or others) in the operational chain of command.

- **Creating New Services, Agencies, and Institutions.** Proposals included elevating U.S. Special Operations Command to a military service rather than a Combatant Command; the creation of a new U.S. cyber service; creating a Remotely Piloted Aircraft agency; and establishing a separate Joint General Staff (in addition to the current Joint Staff) that focuses exclusively on strategic-level issues, reports to CJCS, and has its own career path (rather than drawing personnel from the services). Others recommended against the creation of new services.

- **Revisiting roles and missions.** Proposals included reforming Special Operations Command to become the preferred option for irregular conflict; establishing a commission to review roles and missions for space; shrinking regional Combatant Commands and focusing them on engagement and relationships with foreign counterparts; and creating a better division of labor on irregular warfare.

- Streamlining and improving the decisionmaking by:

  - **Removing unnecessary management layers.** Proposals included consolidating Secretariats and Service Staffs while retaining the Service Secretary positions; reducing the number of management layers in the bureaucracy; encouraging the Department to conduct a top-down de-layering study according to pre-agreed organization design principles, and examining areas of overlap between different DOD components (for example OSD and the Joint Staff) with a view to eliminating redundancy; reducing the number of three- and four-star commands; and eliminating the Joint Requirements Oversight Council.

---

97 U.S. European Command had responsibility for the African theater until 2007, when U.S. Africa Command was founded.
Empowering the DOD workforce. Proposals included increasing the bureaucracy’s autonomy; providing staffs with better training; building greater expertise in the civilian workforce through stopping frequent assignment rotations; and better facilitating horizontal collaboration across DOD components at lower levels than the Office of the Secretary of Defense.

Extending the tenure of the Chairman and Vice Chairman of the Joint Chiefs of Staff. Proposals included shifting from a two-year renewable term to one four-year term or shifting to a five-year (or longer) term.

Managing Costs

Responding to perceptions that DOD has difficulty reigning in its finances and delivering an “appropriate” (however defined) return on its investments, recommendations in this category pertain to perceived issues in the way the Department of Defense accounts for and controls its costs. Since the Department’s establishment, many of its leaders have taken issue with the way the Department manages its finances; a number of reform efforts have therefore been focused on controlling DOD costs and identifying more efficient ways to do business. In terms of recent proposals for reform proposed by defense experts in their testimonies during the first and second sessions of the 114th Congress, areas such as acquisition reform and efforts to improve efficiency, eliminate redundancies, and better prepare defense budgets are included in this group. Recommended changes include the following:

- **Creating Efficiencies**: Proposals included immediately cutting every program behind schedule or over budget; minimizing documentation requirements for program managers; avoiding “gold plating” (shorthand for incorporating costly and unnecessary features) of procurements; shifting jobs from active duty personnel to civilians or contractors; reviewing command relationships for cost savings; reviewing Combatant Command J-8 functions (responsible for evaluating and developing force structure requirements) to avoid duplication; authorizing another round of Base Realignment and Closure (BRAC); and outsourcing depot maintenance.

- **Improving collaboration with industry.** Proposals included loosening requirements to share all relevant information on technologies with commercial analogues with the government; revising contract incentives to reward success and penalize failure; reauthorizing A-76 public-private competitions processes; and encouraging leaders from industry to serve in DOD.

- **Improving business practices.** Proposals included running DOD personnel management like a business; taking more leaders from industry into Pentagon positions; removing requirements for incoming political appointees to divest their assets or equity in companies doing business with DOD; creating greater transparency among stakeholders; changing the measure of a program’s merit from unit cost to cost per effect (i.e., cost per target engaged); establishing a management “reserve” account to address execution risks inherent in every program; and creating a Deputy Secretary position for business transformation.

---

98 Although this report is focused on strategic and organizational reforms to the Pentagon, details on budgetary and financial matters is briefly included due to the fact that observers and policymakers consistently discuss acquisition and cost management as part of the current reform agenda. For more information on this and related topics, see CRS Report R43566, Defense Acquisition Reform: Background, Analysis, and Issues for Congress, by Moshe Schwartz.
Cutting overhead/civilian workforce management. Proposals included establishing a performance management system for civilian employees; creating greater flexibility in civilian pay levels; reducing the civilian workforce but increasing compensation for high-level civilians; cutting the civilian system in half or more; permitting DOD to downsize or eliminate inefficient healthcare systems; combining the Defense Logistics Agency and Transportation Command; and legislating end strengths for military, civilians, and contractors associated with overhead and infrastructure.

Building Capabilities

Other observers have focused on whether DOD is acquiring the right personnel and materiel capabilities, in sufficient quantities and with sufficient readiness to meet 21st century security challenges. Recommendations in this category include suggested augmentations to military personnel management and training; more effectively leveraging emerging technologies; and suggested priority areas for capability development:

- Augmenting military career paths by 99
  - Improving military training and education. Proposals included strengthening top-level (above O-6 & O-6) military education; unifying service professional military education under a joint three-star General or Flag officer; and giving the CJCS authority to direct joint training.
  - Creating more flexibility in military careers. Proposals included giving technical track officers opportunities equal to those of their colleagues in the command track; expanding “early promote” quotas and accelerating rates of advancement; reviewing DOPMA to create a more dynamic management system; making it easier to seek out and promote promising young officers; relaxing joint duty requirements; and shifting requirements for joint credit to O-8 or O-9 levels.
  - Prioritizing key skill sets. Proposals included augmenting the selection and promotion of general and flag officers to prioritize strategic-level thinking; adding psychological resilience to recruiting standards; and developing foreign language requirements for serving in regional combatant commands.
  - Building and leveraging technology by creating processes and systems for rapid prototyping of new capabilities. Proposals included following the JIEDDO model for lower risk technologies,100 and adopting a more tolerant approach to risk and failure on technology development.
  - Revisiting force structure decisions. Proposals included increasing overall military size and end strength; maintaining superiority in undersea and strike warfare, electronic warfare operations, and air warfare; focusing the Marine Corps and United States Special Operations Command on irregular warfare; and focusing the Army on decisive land battle rather than full-spectrum operations.

100 "JIEDDO" stands for Joint Improvised Explosive Device Defeat Organization, which used rapid experimentation and prototyping to develop new battlefield capabilities.
Interagency Reform

A number of observers point out that DOD is but one part of a broader set of U.S. national security institutions. In this view, other institutions (State and USAID, for example) are often better suited to take on security tasks that do not involve the application of military power. Better enabling the United States to grapple with emerging threats may therefore require revisiting interagency national security structures. As one observer noted, “the brokenness of the overall national security system will hamper the effectiveness of U.S. foreign and security policy no matter how well DOD transforms its internal operations or its performance at the operational level of war.” Accordingly, recommendations included in this category were proposals to better synchronize DOD efforts with other U.S. government departments and agencies, and strengthen other, non-DOD national security institutions:

- **Synchronizing DOD activities with those of other USG departments.** Proposals included adjusting Combatant Command headquarters to accommodate increased collaboration with U.S. government agencies and international partners; merging the Department of State and Department of Defense at the regional level; renaming Combatant Commands to “Unified Commands” to signal a whole-of-government approach; expanding the number of State Department foreign policy advisors (or “Political Advisors”) at Combatant Commands; better aligning how the Department of State and DOD divide up geographic regions of the world; and giving regional COCOMs a civilian deputy.

- **Augmenting and strengthening interagency institutions.** Proposals included creating interagency regional centers as regional headquarters for foreign and defense policy; increasing funding for the National Security Council; and designing a “Goldwater-Nichols” act for the interagency. Other observers recommended against such an interagency reform act.

While many of these recommendations are interrelated and could be mutually reinforcing if executed properly, others are in tension with each other. For example, some maintain that adopting proposals currently being tabled such as establishing a Joint General Staff, or placing the Chairman of the Joint Chiefs of Staff in the chain of command, would diminish the Secretary of Defense’s control over the Department of Defense. Another example pertains to more effective interagency collaboration. Some believe that a “Goldwater-Nichols” for the broader, interagency national security establishment is needed in order to better prepare the Department to conduct complex operations. Others believe that top-down interagency organizational reform might be counterproductive.

The Pentagon’s View on Reform Proposals

Using the congressional interest as an impetus, in the fall of 2015 Secretary of Defense Ashton Carter initiated “a comprehensive review of Goldwater-Nichols legislation and related

---


103 Statement of General James L. Jones, Senate Armed Services Committee, December 3, 2015.

104 Vickers, p. 6.
organizational issues in the DOD." To that end, a series of working groups was established in order to "assess key issue areas," and find "additional opportunities for efficiencies and other improvements in the Department's organization." The published results of their deliberations, including recommendations that are supported and not supported by the Department, are organized into the DOD management framework outlined above (the text below is taken directly from the DOD document, with only small alterations for clarification):^107

Formulating Requirements

Actions recommended:

- **Global Integration:** Strengthen the Chairman’s capability to support the Secretary in management, planning, and execution across the Combatant Commands (COCOM). This would be achieved without placing the chairman in the chain of command, through appropriate delegation of authority from the Secretary to the Chairman and to prioritize military activities and resources across COCOM boundaries. The Department will submit legislative proposals clarifying the Secretary’s discretionary authority to delegate such authority to the Chairman.

- **Strategy Development:** Strengthen the capability of the Joint Staff to contribute to strategy development to inform the development of operational plans and the identification of military alternatives to address contingencies, subject to policy guidance and review by the civilian leadership. Improved capabilities should be focused on trans-regional, multi-domain and multi-functional threats, and multiple threats with overlapping timeframes.

- **Streamlined staffing for Regional and Functional Matters:** Review and streamline the organization of DOD “communities of interest” that address regional or functional topics in OSD, Joint Staff, Services, COCOMs and DOD Agencies, to bring together multiple staffs addressing closely related issues, reduce duplication of functions, and better align roles, responsibilities and relationships across the Department.

- **Improved Vertical Integration of Staffs:** Analyze the staffing of functions such as logistics, intelligence and plans in the Joint Staff, the COCOMs, and subordinate commands for potential redundancies and opportunities for savings. This would specifically include consideration of “skipping an echelon” in functional alignment where that can be done without loss of capability.

- **Improved Strategic Guidance Documents:** Review the Department’s strategic guidance documents and the processes for developing them, with goals of providing greater clarity and cohesion, minimizing complexity, and reducing offices that exist to write and staff these documents that are often overlapping and sometimes contradictory. For example, [DOD] will reconsider ... the Defense

---


106 Ibid.

107 Although the content is reorganized into this CRS report’s analytic framework, the actual recommendations are taken verbatim from a DOD memo on the subject. An online copy of the memo can be found here: http://lyxsm73/aop3qvc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2016/04/DoD-G-N-WG-recommendations.pdf.
Strategy Review (formerly known as the Quadrennial Defense Review) the extensive processes used to develop it, most of which duplicate existing strategic planning activities.

- **Elevate Cyber Command (CYBERCOM) to a unified combatant command**, with Title 10/sec 164 authorities to include joint force provider, cyber capabilities advocacy, and theater security cooperation.
  - Retain relationship between CYBERCOM and National Security Agency (NSA). Provide that any separation must be conditions-based, with consideration to (1) separation of personnel and platforms; and (2) institution of mechanisms to ensure NSA continues to respond to COCOM operational requirements as a critical combat support enabler providing strategic and operational threat warning.
  - Maintain current relationships between CYBERCOM and DOD/Service organizations in the near term; assess relationships between cyber organizations to achieve overall mission effectiveness as a follow-on task.
  - Consider organizational and mission changes to rationalize cyber authorities, capabilities, personnel and resources. Examine these potential efficiencies to provide department-wide offset options for $128m 150 billets) over the Future Years Defense Program (FYDP) to make elevation of CYBERCOM resource neutral.

Actions not recommended:

- **Establishment of a General Staff.** The working groups concluded that a General Staff would quickly become a new bureaucracy that is removed from the needs of our fighting forces and less responsive to those needs than the Joint Staff. This view was supported by virtually all of the current and former DOD leaders interviewed by the review team.

- **Inclusion of the Chairman in the Chain of Command.** Placing the Chairman in the chain of command would undermine the principle of civilian control over the military and reduce the Chairman’s ability to provide independent military advice to the President and the Secretary of Defense. The working groups concluded that the capabilities of the Chairman and the Joint Staff could be appropriately enhanced without taking this step.

- **Elimination of COCOM role in warfighting in favor of Joint Task Forces.** The regional combatant commands build strategic relationships with foreign leaders (military and civilian), foster trust, and assure access across their areas of responsibility in a manner that is essential to projecting military power and furthering our policy objectives around the globe. No Joint Task Force could perform its operational mission without the personnel, planning, logistical and communications support provided by the Combatant Commands.

- **Merger of EUCOM and AFRICOM.** AFRICOM was established as a separate unified combatant command less than a decade ago because EUCOM did not have the capacity to address the wide array of military challenges emerging on the African continent. These capacity challenges have not gotten any easier (and in fact have grown more complex) with the increasing Russian threat in Europe and the continuing rise of terrorist threats across Africa.

- **Merger of NORTHCOM and SOUTHCOM.** Central and South America have long felt neglected and ignored by the United States. The existence of
SOUTHCOM is one of the few signals we have given that we care about the region. A merger of NORTHCOM and SOUTHCOM would likely reduce U.S. resources and U.S. influence in the region even further.

- **Merger of DLA and TRANSCOM.** The Department has examined the functions of DLA and TRANSCOM and determined there is minimal overlap between the two. A merger would risk loss of focus on essential missions and a reversal of the substantial progress the Department has made over the last decade in improving the management of these two large businesses.

**Managing Costs**

Actions recommended:

- **Ensure that the Service Chiefs are fully included in the acquisition process by:** (1) requiring the Chiefs to advise the Milestone Decision Authority and concur in cost, schedule, technical feasibility, and performance trade-offs that have been made with regard to the program; and (2) including the Chiefs, or their representatives, on Defense Acquisition Boards for the programs of their services. The Service Chiefs will be responsible and accountable for trade-offs between cost, schedule and performance throughout the life of an acquisition program.

- **Evaluate the feasibility of conducting combined or joint reviews of major Defense Acquisition Programs between the military services and OSD.**

- **Reduce Defense Acquisition Board (DAB) membership.** Current DAB membership includes approximately 35 principal members and advisors, each of whom is likely to feel empowered as a “gatekeeper” for acquisition decisions. The Department will consider combining organizations and realigning membership from individual organizations to functional areas to reduce memberships in order to free up staff time and focus discussions on issues critical to program outcomes.

- **Reduce Acquisition Documentation Touch Points.** The current acquisition process includes 14 documents that must be coordinated by the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD/AT&L) in cases where OUSD/AT&L is the Milestone Decision Authority. The Department will seek opportunities for pushing approval authority down to a lower level in cases where a program remains on course in order to eliminate redundant reviews and shorten review timelines.

- **Streamline documentation** and review processes and examine potential efficiencies from Big Data for acquisition efforts to more effectively address requirements for acquisition data at all levels of the organization.

- **Identify core elements required for developing Capabilities-Based Assessments,** including component-led Study Advisory Groups with external stakeholders, to bolster up front analytic rigor to decisions impacting materiel solutions.

- **Conduct a review of human capital requirements** needed to improve analytical expertise for the identification, assessment, and approval of requirements.
Building Capabilities

Actions recommended:

- **Revise the statutory definition of “joint matters” to broaden the number and type of billets for which an officer may receive joint credit.** Under the current system, for example, a Joint Task Force commander for disaster relief might not be eligible for joint duty credit, while a staff officer serving in a COCOM headquarters would be. The Department will propose revisions that broaden the types of activity for which officers may receive joint credit to include operational and tactical-level experiences that are “joint” in nature.

- **Modify the statutory requirements which prescribe a three-year duty length for all joint duty positions.** The lack of flexibility in the current system effectively precludes some highly qualified officers from competing for command positions in which they are needed. The Department will propose revisions to provide the Secretary with maximum flexibility to recognize intensity and duration of joint duty assignments with the intention of reducing friction with service and individual officer developmental requirements and Defense Officer Personnel Management Timelines.

- **Remove the statutory provisions which require a 10-week, in-residence course, addressing 21 specific issues, to achieve Joint Professional Military Education II accreditation.** These detailed requirements were enacted because the Department resisted the JPME requirement when Goldwater-Nichols was enacted almost 30 years ago and are no longer needed. The Department seeks more flexible and tailor-made delivery methods that will meet Phase II requirements in a manner consistent with JS/Combatant Command (COCOM) needs while maintaining academic rigor.

- **Establish a dedicated program or fellowship experience** to produce joint strategists who are well-credentialed, specifically trained and operationally informed to take part in development, production, and implementation of national military strategy.

Many of these recommendations were subsequently highlighted by Secretary of Defense Carter in a speech at the Center for Strategic and International Studies on April 5, 2016. In his remarks, he stressed that the Department needs better mechanisms to synchronize its global activities, particularly with respect to those issues that cut across the areas of responsibility of the different Combatant Commands. He also sought to codify some of the functions the Chairman of the Joint Chiefs of Staff currently performs. Additional areas for reform highlighted by the Secretary include headquarters staffing reductions and cutting the numbers of four-star officers across the force. Excerpts from the speech wherein he explains his rationale for certain proposals are below (emphasis added):

> accordingly, we need to clarify the role and authority of the Chairman, and in some cases the Joint Chiefs and the Joint Staff, in three ways: one, to help synchronize resources globally for daily operations around the world, enhancing our flexibility, and my ability, to move forces rapidly across the seams between our combatant commands; two, to provide objective military advice for ongoing operations, not just future planning; and three, to advise the Secretary of Defense on military strategy and operational plans, for example, helping ensure that our plans take into account in a deliberate fashion the possibility of overlapping contingencies.
These changes recognize that in today’s complex world, we need someone in uniform who can look across the services and combatant commands and make objective recommendations to the department’s civilian leadership about where to allocate forces throughout the world and where to apportion risk to achieve maximum benefit for our nation. And the person best postured to do that is the Chairman of the Joint Chiefs.

As some of you may know, DoD is currently in the process of reducing our management headquarters by 25 percent—a needed step—and we’re on the road to accomplish that goal thanks to the partnership of the congressional defense committees, which once again we deeply appreciate. We can meet these targets without combining Northern Command and Southern Command, or combining European Command and Africa Command—actions that would run contrary to why we made them separate, because of their distinct areas of emphasis and increasing demands on our forces in them. And indeed those demands have only further increased in recent years, with each command growing busier. So instead of combining these commands to the detriment of our friends, our allies, and in fact our own command and control capabilities, we intend to be more efficient by integrating functions like logistics, intelligence, and plans across the Joint Staff, the combatant commands, and subordinate commands, eliminating redundancies while not losing capability, and much can be done here.

Additionally, in the coming weeks the Defense Department will look to simplify and improve command and control where the number of four-star positions have made headquarters either top-heavy, or less efficient than they could be. The military is based on rank hierarchy, where juniors are subordinate in rank to their seniors; this is true from the platoon to the corps level, but it gets complicated at some of our combatant and component command headquarters, where we have a deep bench of extremely talented senior leaders. So where we see potential to be more efficient and effective, billets currently filled by four-star generals and admirals will be filled by three-stars in the future.

The next area I want to discuss today is acquisition.... One way we’re improving is by involving the service chiefs more in acquisition decision-making and accountability, consistent with legislation Congress passed last year—including giving them a seat on the Defense Acquisition Board, and giving them greater authority at what’s known as “Milestone B,” where engineering and manufacturing development begins; that is, where programs are first defined and a commitment to fund them is made... Another way we’ll seek to improve is by streamlining the acquisition system itself. This will include evaluating and where appropriate reducing other members of the Defense Acquisition Board.[,]

... as we’ve learned over the years what it takes to operate jointly, it’s become clear that we need to change the requirements for joint duty assignments, which are more narrow and rigid than they need to be. Accordingly, we’re proposing to broaden the definition of positions for which an officer can receive joint duty credit, going beyond planning and command-and-control to include joint experience in other operational functions, such as intelligence, fires, transportation and maneuver, protection, and sustainment, including joint acquisition.108

Reactions to the proposals put forward by Secretary Carter have been mixed. Some observers describe these initiatives, when taken together, as an “aggressive” change to the Pentagon’s organization, and the most sweeping package of reforms suggested in decades.109 Others take a


109 Ryan Faith, “Secretary of Defense Ash Carter Wants to Fix Everything Wrong With The Pentagon,” Vice News, (continued...)

Congressional Research Service
more skeptical view, noting that the package of recommendations proposed by the Pentagon represents incremental changes. In this view, these changes are perhaps necessary, but not sufficient, to prepare the Department to meet emerging strategic challenges. Among those with this view reportedly is Senate Armed Services Committee Chairman John McCain, who noted to the press that his suggested changes to the way the Department does business will be "more comprehensive and more controversial." Finally, some observers believe that an incremental approach to changing the Department is preferable absent a common diagnosis of the challenges beleaguering the Pentagon.

Recent Legislation on Defense Reform

The House Armed Services Committee formally expressed its diagnosis of the defense reform challenge in H.Rept. 114-537, stating

The committee recognizes that security challenges have become more transregional, multi-domain, and multi-functional; that U.S. superiority in key warfighting areas is at risk with other nations' technological advances; and that the Department of Defense lacks the agility and adaptability necessary to support timely decisionmaking and the rapid fielding of new capabilities. The proposals contained in this subtitle are focused on increasing accountability and oversight, enhancing global synchronization and joint operations, and strengthening strategic thinking and planning, while preserving civilian control of the military and the role of the Chairman of the Joint Chiefs of Staff as the principal, independent military advisor to the President and the Secretary of Defense.

While the Senate Armed Services Committee declined to state its formal view on the overall goals for its defense reform agenda in S.Rept. 114-255, Chairman John McCain has previously noted

The focus of Goldwater-Nichols was operational effectiveness, improving our military's ability to fight as a joint force. The challenge today is strategic integration. By that, I mean improving the ability of the Department of Defense to develop strategies and integrate military power globally to confront a series of threats, both states and non-state actors, all of which span multiple regions of the world and numerous military functions.

This sentiment appears to provide a logical underpinning for a number of the defense reform proposals presented in S. 2943.

The following table organizes the various legislative proposals included in "Title IX—Department of Defense Organization and Management" sections of both H.R. 4909 and S. 2943. As the

(...continued)


111 Ibid.


Obama Administration did not send formal legislative proposals to Congress to inform these debates, when possible and appropriate the table refers to recommendations formulated by DOD in conjunction with its own Goldwater-Nichols review.\textsuperscript{115}

\textbf{Table 1. Select DOD Reform Proposals}

<table>
<thead>
<tr>
<th>HASC-Reported Bill (H.R. 4909)</th>
<th>SASC-Reported Bill (S. 2943)</th>
<th>Administration Recommendations (Goldwater-Nichols Working Group Memo)\textsuperscript{a}</th>
<th>Conference Report</th>
</tr>
</thead>
</table>
| \$902 & \$903 Eliminate the Quadrennial Defense Review (QDR) and Defense Strategy Review (DSR) processes and replaces them with:  
  - top-down strategic guidance on force structure and priorities from the Secretary of Defense, issued every four years;  
  - annual policy guidance to DOD components for their preparation and review of program recommendations and budget proposals; and  
  - a new, independent commission on the National Defense Strategy of the United States. | \$921 Augments CJCS responsibilities in strategy formulation, to include  
  - develop strategic frameworks and plans to guide the use of military force across all regions, military functions, and domains;  
  - advise the Secretary of Defense (SecDef) on production of national defense strategy and national security strategy;  
  - provide advice to the President and SecDef on ongoing military operations;  
  - prepare alternative military analysis, options, and plans to recommend to SecDef, as CJCS considers appropriate;  
  - prepare joint logistic, mobility, and operational energy plans to support the national defense strategy; and  
  - provide for preparation and review of contingency plans. | “Strengthen the capability of the Joint Staff to contribute to strategy development to inform the development of operational plans and the identification of military alternatives to address contingencies, subject to policy guidance and review by the civilian leadership. Improved capabilities should be focused on trans-regional, multi-domain and multi-functional threats, and multiple threats with overlapping timeframes.” | N/A |
| \$905 Requires that the National Military Strategy, as prepared by the CJCS  
  - develops the military ends, ways, and means to support national | \$921 Recalibrates the National Military Strategy as prepared by CJCS, including a requirement to identify the priority of joint force capabilities, capacities, and resources, as well as establish | “Review the Department’s strategic guidance documents and the processes for developing them, with goals of providing greater clarity and | |

<table>
<thead>
<tr>
<th>HASC-Reported Bill (H.R. 4909)</th>
<th>SASC-Reported Bill (S. 2943)</th>
<th>Administration Recommendations (Goldwater-Nichols Working Group Memo)(^*)</th>
<th>Conference Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>objectives;</td>
<td>military guidance for the development of the joint force.</td>
<td>cohesion, minimizing complexity, and reducing offices that exist to write and staff these documents that are often overlapping and sometimes contradictory. For example, [DOD] will reconsider ... the Defense Strategy Review (formerly known as the Quadrennial Defense Review) the extensive processes used to develop it, most of which duplicate existing strategic planning activities.”</td>
<td></td>
</tr>
<tr>
<td>• assesses strategic and military risks, including risk mitigation options;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• establishes a strategic framework for development of operational and contingency plans;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• prioritizes joint force capabilities, capacities, and resources; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• establishes military guidance for the employment of the joint force.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

§906 Updates requirement in P.L. 114-92 §1064 (b)(2) for an independent study of national security strategy formulation to include workforce ability to conduct strategic planning.

§904 Requires the Secretary of Defense prepare policy guidance on contingency planning at least every two years, and submit that guidance to relevant congressional committees.

---

**Office of the Secretary of Defense (OSD) Management**

| N/A | §901 Redesignates Under Secretary of Defense (USD) Business Management and Information to USD Management & Support and adds responsibilities to the position, including oversight of agencies associated with execution of acquisition functions. | “Review and streamline the organization of DOD ‘communities of interest’ that address regional or functional topics in OSD, Joint Staff, Services, COCOMs and DOD agencies, to bring together multiple staffs addressing closely related issues, reduce duplication of functions, and better align roles, responsibilities and relationships across the Department.” N/A |

---

Congressional Research Service

380
<table>
<thead>
<tr>
<th>HASC-Reported Bill (H.R. 4909)</th>
<th>SASC-Reported Bill (S. 2943)</th>
<th>Administration Recommendations (Goldwater-Nichols Working Group Memo)</th>
<th>Conference Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>§903 Establishes an Assistant Secretary of Defense for Information (Chief Information Officer) in OSD, responsible for cyber and space policy, information network defense, policies and standards governing information technology systems and related activities across DOD.</td>
<td>§906 Establishes a 30-person defense management reform and business transformation unit to help senior managers develop management reform roadmaps and monitor their implementation.</td>
<td>§923 Modifies the roles and responsibilities of Assistant Secretary of Defense for Special Operations/Low Intensity Conflict to have overall supervision of special operations activities within DOD, and to allow it to better perform service secretary-like functions.</td>
<td>§923 Creates Special Operations Functional Integration and Oversight Teams to integrate functional activities of DOD to provide capabilities required for special operations missions.</td>
</tr>
<tr>
<td>§941 Requires SecDef to establish “cross-functional mission teams” on priority issue areas to produce comprehensive and fully integrated policies, strategies, plans, and resourcing and oversight.</td>
<td>§941 Requires SecDef issue a directive on the purposes, values, and principles for the operation of OSD, as well as a directive on collaborative behavior. Also ties career progression to collaborative behavior.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HASC-Reported Bill (H.R. 4909)</td>
<td>SASC-Reported Bill (S. 2943)</td>
<td>Administration Recommendations (Goldwater-Nichols Working Group Memo)*</td>
<td>Conference Report</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>§941 Requires SecDef to take actions to streamline the organizational structure of OSD to increase spans of control, reduce management layers, and eliminate unnecessary duplication between OSD and the Joint Staff.</td>
<td>§941 Mandates that positions requiring advice and consent of the Senate successfully complete a course of instruction on leadership, modern organizational practice, collaboration, and the operation of mission teams (described earlier in the act).</td>
<td>§942 Requires SecDef formulate and implement management strategies through 2022 on human capital, personnel cost savings targets, elimination of functions, force management authorities, and de-layering of organizations.</td>
<td></td>
</tr>
</tbody>
</table>

**Chairman of the Joint Chiefs of Staff (CJCS) Authorities and Responsibilities**

| §907 Extends length of CJCS tour from two to four years, in a manner designed to bridge Administrations. | §921 Extends length of CJCS tour from two to four years, beginning on an odd-numbered year, with a possible two-year further extension. | “Strengthen the Chairman’s capability to support the Secretary in management, planning, and execution across the Combatant Commands (COCOM). This would be achieved without placing the chairman in the chain of command, through appropriate delegation of authority from the Secretary to the Chairman and to prioritize military activities and resources across COCOM boundaries.” | N/A |

**Congressional Research Service**

38
<table>
<thead>
<tr>
<th>HASC-Reported Bill (H.R. 4909)</th>
<th>SASC-Reported Bill (S. 2943)</th>
<th>Administration Recommendations (Goldwater-Nichols Working Group Memo)*</th>
<th>Conference Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>§908 Codifies CJCS role in advising the President and SecDef on ongoing military operations, as well as the allocation and transfer of forces among geographic and functional combatant commands to address transregional, multi-domain, and multi-functional threats.</td>
<td>§921 Amends Title X U.S.C., Section 153 by codifying primary focus of CJCS as developing military elements of national and defense strategy, assisting the President and SecDef in integration of military operations and activities worldwide, and advocating for current and future joint force requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>§921 Paragraph (4) amends Title X, U.S.C. §153 by establishing a new joint capability development role for CJCS.</td>
<td>§922 Allows SecDef to delegate some authority to CJCS for the worldwide reallocation of limited military assets on a short-term basis.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>§921 Extends the term of service for VCJCS from two to four years, specifies that VCJCS is not eligible for promotion to any other position in the armed forces, and requires VCJCS appointment not take place in same year as CJCS appointment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HASC-Reported Bill (H.R. 4909)</td>
<td>SASC-Reported Bill (S. 2943)</td>
<td>Administration Recommendations (Goldwater-Nichols Working Group Memo)*</td>
<td>Conference Report</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>§910 Reduces the number of general and flag officer positions by five.</td>
<td>§904 Augments Title X, U.S.C. by placing a 15% growth cap on numbers of personnel assigned to Army, Navy, and Air Force staffs in times of war.</td>
<td>“Analyze the staffing of functions such as logistics, intelligence and plans in the Joint Staff, the COCOMs, and subordinate commands for potential redundancies and opportunities for savings. This would specifically include consideration of ‘skipping an echelon’ in functional alignment where that can be done without loss of capability.” Secretary Carter also stated at CSIS that: “the Defense Department will look to simplify and improve command and control where the number of four-star positions have made headquarters either top-heavy, or less efficient than they could be.”</td>
<td></td>
</tr>
<tr>
<td>§910 Requires that the rank of a commander of a service or functional component command under a combatant command be no higher than lieutenant general or vice admiral.</td>
<td>§904 Reduces number of General and Flag Officers that can be assigned to military departments.</td>
<td>§905 Limits use of funds for contractors for staff augmentation at DOD headquarters and military departments.</td>
<td></td>
</tr>
<tr>
<td>§911 Augments the Unified Command Plan by elevating U.S. Cyber Command (CYBERCOM) to a unified command.</td>
<td>§921 Requires C/JCS to recommend budget proposals for each combatant command, establish a uniform system for evaluating COCOM preparedness, and advise SecDef on the extent to which major programs and policies support national defense strategy and COCOM contingency plans.</td>
<td>“Elevate Cyber Command (CYBERCOM) to a unified combatant command, with Title 10/sec 164 authorities to include: joint force provider, cyber capabilities advocacy, and theater security cooperation.”</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Combatant Commands (COCOMs)**
<table>
<thead>
<tr>
<th>HASC-Reported Bill (H.R. 4909)</th>
<th>SASC-Reported Bill (S. 2943)</th>
<th>Administration Recommendations (Goldwater-Nichols Working Group Memo)*</th>
<th>Conference Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>§914 Requires SecDef contract an independent entity to assess COCOM structures and recommend areas for improvement.</td>
<td>§921 Requires COCOM commanders consult with CJCS in the performance of their duties.</td>
<td>§921 Establishes a provision in Title X U.S.C. specifying the primary duties of combatant commanders, focusing on planning for employment of forces, responding to significant military contingencies, and deterring conflict.</td>
<td>§921 Establishes a Combatant Commanders Council to inform requirements, production periodic review, and implementation of the national defense strategy (NDS) and to assist SecDef with global integration of military operations.</td>
</tr>
<tr>
<td>§923 Clarifies the administrative chain of command for SOCOM.</td>
<td>§923 Gives the Commander, USSOCOM the authority to monitor promotions of special operations forces and coordinate with military departments regarding assignment, retention, training, professional military education, and special and incentive pays of special operations forces.</td>
<td>§924 Requires SecDef carry out a pilot program to organize subordinate commands of a unified combatant command around joint task forces rather than through service component commands.</td>
<td>§925 Expands eligibility for Deputy Commanders of COCOMs that have the United States among their geographic areas of responsibility to include officers from the reserves.</td>
</tr>
</tbody>
</table>
# Issues for Congress

As the debate on reforming the Department of Defense begins to take shape, Congress may consider the following questions:

- What kinds of characteristics must DOD have if it is to be able to effectively respond to the nation’s current and future national security challenges? Is improved global synchronization, as proposed by the DOD, sufficient to enable DOD to achieve desired characteristics (e.g., agility or innovativeness)?
• Will the proposed changes to DOD’s structures and processes enable the Department to achieve the overall aim of strengthening strategic integration and strategic planning? Will they enable the DOD to be more flexible and agile?
• What might be some of the unintended consequences of each reform proposal? How might those be mitigated?
• What kinds of missions are national leaders likely to require U.S. military forces to perform? Is the Department configured in a manner that enables the performance of those missions? Should other government departments perform certain critical tasks currently being performed by DOD?
• Will reforming DOD sufficiently enable the United States to grapple with emerging national security challenges, or is a broader examination of the interagency national security architecture required?
• What processes within the Department are working well? Which are not working well? What functions are currently accomplished by working outside existing or established DOD processes?
• What changes to DOD’s culture might be necessary to foster a climate of innovation and experimentation?
• What, if anything, might be done to improve the quality of military and strategic advice delivered to senior defense and national security leaders?
Appendix. Select Defense Management and Organizational Reform Proposals since the 1980s

Over DOD’s history, reform efforts have tended to be prompted when leaders in the executive branch or Congress perceive deficiencies in the way that the Department formulates requirements, build capabilities, or manages its costs. For example, cost overruns in the 1980s led the Reagan Administration to establish the Packard Commission, tasked with identifying ways to improve efficiency across the government, with particular attention paid to DOD. Simultaneously, congressional concern that DOD was failing to build the institutional capabilities necessary to effectively prosecute joint operations led to the Goldwater-Nichols Reform Act of 1986. After the end of the Cold War, concerns that DOD strategy was no longer keeping pace with changing strategic realities led to the formulation—and institutionalization—of the Quadrennial Defense Review (QDR) process; concerns that the QDR was not effectively articulating and accounting for U.S. national security risks led Congress to reform the quadrennial strategy process (now called the Defense Strategy Review) in the FY2015 NDAA (P.L. 113-291).

Key reform initiatives and proposals, with particular emphasis on reforms and changes to defense strategy, management, and organization, since 1980 include the following:

1983-1984—President’s Private Sector Survey on Cost Control (The “Grace Commission”)

On June 30, 1982, President Reagan signed Executive Order 12369 formally establishing the President’s Private Sector Survey on Cost Control in the Executive Branch. An Executive Committee under the chairmanship of J. Peter Grace was established, consisting of 161 high-level private sector executives—mostly chairmen and chief executive officers—from many of the nation’s leading corporations. The report delivered nearly 2,500 recommendations to President Reagan to improve efficiency and deliver cost savings across the executive branch. With respect to Defense specifically, in June 1983 the Grace Commission stated that the Department of Defense could save $92 billion over three years by reducing major weapon purchases, closing military commissaries in the United States, consolidating or shutting down military bases, and reforming the military health care system. The Grace Commission also identified federal retirement programs, specifically including the uniformed services retirement system, as potential sources of substantial cost savings. It also proposed alternatives formulated solely on the basis of cost savings rather than on uniformed services manpower force requirements. President Reagan endorsed, and implemented, a large proportion of the Commission’s recommendations across the executive branch. As a result, the DOD’s acquisition system was improved, the Department of Veteran’s Affairs health system was overhauled, and the Base Realignment and Closure process closed dozens of facilities.

1985—“Defense Organization: The Need for Change”

In January 1985, Senators Barry M. Goldwater and Samuel A. Nunn (chairman and ranking Member of the Senate Armed Services Committee respectively) reinvigorated a defense reform study initially directed in June 1983 by their respective predecessors. James Locher, committee staff member and study director, submitted a 645-page study, entitled “Defense Organization: The

116 The President’s Private Sector Survey on Cost Control, January 12, 1984.
Need for Change,” on October 16, 1985. SASC began a 10-day series of hearings on DOD reform that same date; Locher’s findings informed those deliberations. The study identified 16 key problems with the Department and its operations:

- Limited mission integration at DOD’s policymaking level;
- Imbalance between service and joint interests;
- Imbalance between modernization and readiness;
- Inter-service logrolling;
- Inadequate joint advice;
- Failure to implement adequately the concept of unified command;
- Unnecessary staff layers and duplication of effort in the top management headquarters of the military departments;
- Predominance of programming and budgeting;
- Lack of clarity of strategic goals;
- Insufficient mechanisms for change;
- Inadequate feedback;
- Inadequate quality of political appointees and joint duty military personnel;
- Failure to clarify the desired division of work;
- Excessive spans of control;
- Insufficient power and influence of the Secretary of Defense; and
- Inconsistent and contradictory pattern of congressional oversight.

Of the 91 recommendations that Locher made in order to address this problem, the 12 generally deemed most important were the following:

- Establish three mission-oriented Under Secretary positions in the Office of the Secretary of Defense for (a) nuclear deterrence; (b) NATO defense; and (c) regional defense and force projection.
- Disestablish the Joint Chiefs of Staff and, thereby, permit the Service Chiefs to dedicate all their time to service duties.
- Establish a Joint Military Advisory Council consisting of a Chairman and a four-star military officer from each service on his last tour of duty to serve as principal military advisors to the President, the National Security Council, and the Secretary of Defense.
- Authorize the Chairman of the Joint Military Advisory Council to provide military advice in his own right.
- Designate one of the members of the Joint Military Advisory Council, from a different service pair (Army/Air Force and Navy/Marine Corps) than the Chairman, as Deputy Chairman.
- Specify that one of the responsibilities of the Joint Military Advisory Council is to inform higher authority of all legitimate policy alternatives.
- Authorize the Chairman of the Joint Military Advisory Council to develop and administer a personnel management system for all military officers assigned to joint duty.
- Establish in each service a joint duty career specialty.
• Make the Chairman of the Joint Military Advisory Council (JMAC) the principal military advisor to the Secretary of Defense on operational matters and the sole command voice of higher authority within the JMAC system while ensuring absolute clarity that the JMAC Chairman is not part of the chain of command.

• Remove the service component commanders within the unified commands from the operational chain of command.

• Fully integrate the Secretariats and military headquarters staffs in the Departments of the Army and Air Force and partially integrate the Secretariat and military headquarters staffs in the Department of the Navy (the Department of the Navy is treated differently because of its dual-service structure).

• Create the position of Assistant Secretary of Defense (Strategic Planning), who would be responsible for establishing and maintaining a well-designed and highly interactive strategic planning process.  

While the study proposed some radical changes, only a few of them were adopted, mostly in the areas of personnel management and the chain of command, through the Goldwater-Nichols legislation (see below).

1986 — The Packard Commission

President Ronald Reagan established his Blue Ribbon Commission on Defense Management on July 15, 1985. The commission, which was headed by David Packard (founder of Hewlett-Packard and former Deputy Secretary of Defense), was instructed to “study defense management policies and procedures, including the budget process, the procurement system, legislative oversight, and the organizational and operational arrangements, both formal and informal, among the Office of the Secretary of Defense, the Organization of the Joint Chiefs of Staff, the Unified and Specified Command system, the Military Departments, and the Congress.” While the study explored many facets of the DOD and its management, the overall objective was to identify efficiencies and associated cost savings. Ultimately, the commission found that “establishment of strong centralized policies implemented through highly decentralized management structures” would improve DOD’s efficiency and effectiveness. The recommendations themselves were organized into four areas: national security planning and budgeting; military organization and command; acquisition organization and procedures; and government-industry accountability. The report noted:

Meeting these challenges will require, we believe, a rededication by all concerned to some basic principles of management. Capable people must be given the responsibility and authority to do their job. Lines of communication must be kept as short as possible. People on the job must be held accountable for results. These are the principles that guide our recommendations on defense organization and acquisition. They apply whether one is fighting a war or managing a weapons program.

Many of the Packard report’s recommendations pertained to defense acquisition; of note, it argued for the creation of two-year defense budgets in order to find efficiencies in the defense program through fiscal stability. This recommendation was somewhat implemented in the 1986


Defense Authorization Act, which required DOD submit two-year budgets to Congress. However, DOD never received both authorizations and appropriations to cover this biennial period and therefore the Department had to submit an additional one-year budget to the second session of Congress.¹²⁰ This biennial budgetary provision was repealed in the FY2008 NDAA.


President Ronald Reagan established his Blue Ribbon Commission on Defense Management on July 15, 1985 (discussed below). One month after President Ronald Reagan received the Packard Commission’s interim report he issued NSDD 219 in order to implement the Commission’s findings. Key provisions included the following:

- Improving the integration of national security strategy with fiscal guidance provided to the Department of Defense. This included issuing provisional five-year budget levels to DOD; developing procedures for producing a military strategy to support national objectives; a net assessment of military capabilities; and the selecting by the President of a military program and the associated budget level.

- Strengthening military command, control, and advice. This included improving procedures for the Chairman, Joint Chiefs of Staff to channel the reports of the Combatant Commanders to the Secretary of Defense and channel presidential and Secretary of Defense orders to the Combatant Commanders; revising the Unified Command Plan and other related publications to provide broader authority to the Combatant Commanders to structure subordinate commands, joint task forces, and support activities; providing options on Combatant Command (CoCom) organizational structures to accommodate the “shortest possible” chain of command; increasing flexibility to deal with situations that overlap CoCom geographical boundaries; and repealing the statutory provision against the establishment of a single Unified Command for transportation.

- Improving Acquisition Management. Anticipating the establishment of a new Under Secretary of Defense for Acquisition, NSDD 219 directed the Secretary of Defense to develop a directive outlining the roles and responsibilities of the new Under Secretary, to include defining the scope of the “acquisition” function; setting policy for procurement and research and development; supervising of the entire Department acquisition system; establishing policy for oversight of defense contractors; and developing appropriate guidance for auditing defense contractors.

1986 — Goldwater-Nichols Act¹²²

The Goldwater-Nichols Act was the first major defense organizational reform legislation since the Defense Reorganization Act of 1958. Building on the results of its own investigations, as well as Packard Commission findings, Congress sought to address what it believed were fundamental systemic problems in DOD. These included serious organizational defects in the organization of

the Joint Chiefs of Staff, an inability of the military services to work together, a lack of mission focus in the Office of the Secretary of Defense, weaknesses in the budget process, and deficiencies in congressional oversight of DOD programs and plans. Its five main titles dealt with the organization of DOD, including the Office of the Secretary of Defense, and the powers and duties of the Secretary; the Joint Chiefs of Staff and the combatant commands; defense agencies and field activities; joint officer personnel policy; and the military departments. The Goldwater-Nichols Act, which was resisted by members of the Administration and the military, specifically focused on areas for improving “jointness” among the military services.

In late 1986, Senators Nunn and Cohen introduced legislation to promote jointness for the Special Operations Community. The resulting public law amended the Goldwater-Nichols Act by establishing a four-star Special Operations combatant command, as well as an Assistant Secretary position within the Office of the Secretary of Defense responsible for Special Operations/Low Intensity Conflict.

1989—Defense Management Review

In February 1989, President George Bush addressed a joint session of Congress, announcing he was directing the Secretary of Defense to develop a plan to improve the defense procurement process and management of the Pentagon, and to “accomplish full implementation of the recommendations of the Packard Commission and to realize substantial improvements in defense management overall.” Key recommendations included the following:

- Achieving better management of defense agencies and components through better synchronization of senior leaders’ roles and responsibilities, and by assigning overall responsibility for DOD’s day to day management, operations, and the Planning, Programming, and Budgeting System (PPBS) to the Deputy Secretary of Defense;
- Establishing a Defense Executive Committee of DOD senior leadership, replacing the Defense Resources Board with a Defense Planning and Resources Board;
- Better prioritizing programs and incorporating alternative planning scenarios in the PPBS, thereby making it more responsive to emerging requirements while operating on a two-year budgeting cycle (consistent with Packard Commission recommendations) in order to achieve better programmatic stability;
- Streamlining acquisition and procurement processes;
- Reducing the acquisition workforce and requiring each military service to submit plans for a dedicated corps of officers who would make a full-time career as acquisition specialists;
- Streamlining the number of directives and issuances associated with acquisition; and
- Improving logistics management, to include reducing supply, repair parts, and transportation costs.

The report also suggested several legislative changes, particularly pertaining to acquisition.

124 Ibid., p. 1.
1992—Base Force Review

Developed under then-Chairman of the Joint Chiefs of Staff Colin Powell, the “Base Force” Review was an initiative to understand the minimum required force structure for the emerging post-Cold War security environment. Although the Base Force Review was presented to Congress in 1991, it was not until the 1992 National Military Strategy (NMS) was released that its full implications would become clear. The 1992 NMS identified four “foundations” for national military strategy: strategic deterrence and defense; forward presence; crisis response; and reconstitution (or, the capacity to rebuild forces if necessary). U.S. force structure would be designed to accomplish these tasks and advance U.S. interests in regions vital to the United States, rather than on the basis of fighting multiple major regional conflicts (as later defense plans would argue for). Three force packages comprised the core of the Base Force’s conventional structure:

- **Atlantic forces.** To meet threats and secure interests across the Atlantic in Europe, Southwest Asia, and the Middle East. These forces were to be “heavy,” and were to have a significant reserve component.
- **Pacific forces.** These forces were to advance U.S. interests in East Asia and the Pacific. Pacific forces were to be “light” and predominantly maritime, and were to include some Army and Air Force forward-deployed presence, and less of a reserve component than the Atlantic forces.
- **Contingency forces.** These were to consist of light, mobile forces that were CONUS-based and “ready to go on a moment’s notice.” These rapidly mobile, highly lethal forces were seen as likely to serve as the leading edge of forces being introduced for major regional contingencies and were to be less reliant on reserve components than the Atlantic and Pacific forces.

Thus, the “Base Force” would comprise 20 Army Divisions (12 active, 6 reserve, and 2 reserve cadre divisions); 26.5 USAF tactical fighter wing equivalents (15.25 active, 11.25 reserve); 4 Marine Expeditionary Forces (MEFs); and 12 Navy carriers. These force packages entailed a reduction in major force elements and manpower ranging from 20% to 40%, depending on service/component (with an approximate 25% reduction Department-wide). With respect to acquisition, longer-term investment accounts were prioritized while procurement spending declined in order to meet top-line defense spending reductions.

1993—Chairman of the Joint Chiefs of Staff Report on the Roles, Missions, and Functions of the U.S. Armed Forces\(^{125}\)

Informed by the findings of the Base Force Review, in February 1993, Chairman of the Joint Chiefs of Staff Colin Powell released a roles and missions report. Key recommendations included

- removing any and all Marine Corps and Army requirements for nuclear forces;
- closing some 800 bases overseas and cutting of some 100 defense acquisition programs;
- putting forces based in the United States under a Joint command (Atlantic Command); and

• placing U.S. Space Command under U.S. Strategic Command.

1993—The Bottom-Up Review (BUR)\textsuperscript{126}

In order to further reorient the Department away from the Cold War threat environment, in 1993 Secretary of Defense Les Aspin directed a comprehensive review of the “nation’s defense strategy, force structure, modernization, infrastructure and foundations.” The Bottom-Up Review (BUR) sought to find further efficiencies (the “peace dividend”) while simultaneously reconceptualizing the threat environment in which U.S. forces would be required to operate. The BUR organized the Department and its capabilities into four “building blocks”:

• **Major regional contingencies.** This pertained to the U.S. ability to fight a major regional conflict against a substantial regional threat. The operational concept for this kind of campaign was broken into four phases: (1) halt an invasion; (2) build up U.S. combat power in the region while reducing the enemy’s ability to operate; (3) decisively defeat the enemy; and (4) provide for post-war stability.

• **Peace enforcement and intervention operations.** This block was to be capable of forcing entry into, seizing, and holding key facilities; controlling troop and supply movements; establishing safe havens; securing protected zones from internal threats such as snipers, terrorist attacks, or sabotage; and preparing the environment for relief by peacekeeping units or civilian authorities.

• **Overseas presence operations.** This block was designed to deter adventurism and coercion by potentially hostile states, reassure friends, enhance regional stability, and underwrite a larger strategy of international engagement, prevention, and partnership. It also was to help improve U.S. ability to respond effectively to crises or aggression, provide the leading edge of a rapid response capability needed in a crisis, and improve interoperability.

• **Address Nuclear Dangers.** This block included activities associated with reducing the threat of WMD use by adversaries against the United States and its interests. In addition to retaining the capacity for nuclear retaliation against those who might use WMD against the United States, other activities included cooperative threat reduction, nuclear nonproliferation, counter-proliferation, and active and passive defenses against nuclear, biological, and chemical weapons and their delivery systems.

The BUR also stipulated a further reduction in forces from FY1990, seeking to reduce the size of the Armed Forces by approximately 33%—well beyond the Base Force’s planned overall 25% force reduction.

1995—Commission on the Roles and Missions of the Armed Forces\textsuperscript{127}

John P. White, former Assistant Secretary of Defense from 1977 to 1978, chaired the Commission on Roles and Missions, which issued its report, Directions for Defense, in May 1995. It concluded that in the 21st century, every DOD element must focus on supporting the operations of the Unified Commanders in Chief (CINCs)—now referred to as Combatant Commanders (CoCOMs). Recommendations were designed to strengthen this support and included


• Improving Jointness. The Chairman of the JCS should propose to the Secretary of Defense a unified vision for joint operations to guide force and materiel development; integrate support to CINCs in such critical areas as theater air/missile defense and intelligence; improve joint doctrine development; develop and monitor joint readiness standards; and increase emphasis on joint training;

• Elevating CINCs. Larger roles for the CINCs in structuring and controlling command, control, and intelligence support; joint training; and theater logistics;

• Establish a new “Jointness” CINC. Creation of a new, functional unified command responsible for joint training and integration of all forces based in the continental United States (note, this resulted in the re-designation of Atlantic Command as U.S. Joint Forces Command);

• Planning for Peace Operations. Differentiating peace operations from “operations other than war” (OOTW) in order to give them greater prominence in contingency planning;

• Increasing service focus on “core competencies.” Rather than attempt to eliminate duplication of assets between services (i.e., eliminate the “four air forces” problem), the report found that existing problems with service roles are symptoms of the need for DOD to concentrate more intensely on unified operations;

• Improving Health Care. Giving beneficiaries of DOD health care more choice between military and civilian care; and

• Improving Acquisition Infrastructure. Rejecting a “monolithic” acquisition organization independent of the services, as it could undermine core combat capabilities. Instead, infrastructure supporting the purchase and maintenance of equipment should be improved.

The report also called for better DOD coordination with other USG agencies for tasks including combating proliferation of weapons of mass destruction, information warfare, operations other than war, and in overall national security strategy development.

1996—Joint Vision 2010\textsuperscript{128}

In 1996, Chairman of the Joint Chiefs of Staff Shalikashvili issued a “conceptual template for how America’s Armed Forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting.”\textsuperscript{129} While not a Secretary of Defense or congressionally mandated reform initiative per se, the document formed the intellectual foundation for subsequent defense organization reform proposals through the remainder of the Clinton Administration. The vision of future warfighting that Shalikashvili proposed “embraces information superiority and the technological advances that will transform traditional warfighting via new operational concepts, organizational arrangements, and weapons systems.”\textsuperscript{130} In other words, Joint Vision 2010 explored the ways in which the United States military might build upon—and take advantage of—its technological superiority (the “Revolution in Military Affairs”). The necessity of building and exploiting U.S. technological advantage in the


\textsuperscript{129} Ibid., p. 1.

battle space subsequently became a key concept in defense strategy and planning, especially as it enabled (at least in theory) force structure reductions through improving effectiveness of the joint force.

1997—Quadrennial Defense Review\textsuperscript{131}

The 1997 Quadrennial Defense Review, which was congressionally mandated, embraced the notion of defense transformation (or, the adoption of, and investment in, technology to improve the manner in which the United States conducts its military operations). In particular, it argued for improving command and control capabilities through advanced command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architectures. It also noted the Department’s intent to leverage new technologies to harness the “Revolution in Military Affairs” through new operational concepts, doctrine, and organizational changes. This QDR reaffirmed the “two major theater war” force sizing construct, and accordingly justified the need to retain a nuclear deterrent based on a triad of forces, as well as to retain 10 Army divisions, 12 aircraft carriers, 20 fighter wings, and 3 Marine Expeditionary Forces. It also reaffirmed the requirement to keep approximately 100,000 personnel forward deployed both in Europe and in the Pacific and to regularly deploy naval, air, ground, and amphibious forces around the world. Additional recommendations included

- Further reducing civilian and military personnel associated with infrastructure beyond the initiatives in the DOD budget for FY1998 by 109,000, bringing the total reduction to infrastructure employment since 1989 to 39%;
- Requesting authority for two additional rounds of BRAC, one in 1999 and the second in 2001;
- Improving efficiency and performance of DOD support activities by adopting innovative management and business practices of the private sector. These include “reengineering” or “reinventing” DOD support functions, for example, streamlining, reorganizing, downsizing, consolidating, computerizing, and commercializing operations;
- Considering far more non-warfighting DOD support functions as candidates for outsourcing—inviting commercial companies to compete with the public sector to undertake certain support functions.\textsuperscript{132}

Other recommendations in the QDR were included in the Defense Reform Initiative.

1997—Defense Reform Initiative\textsuperscript{133}

Based on the findings of the 1997 Quadrennial Defense Review (QDR) Process, Secretary of Defense William Cohen established a Task Force on Defense Reform to find ways to improve the organization and procedures in the Department. It was asked to recommend organizational reforms, reductions in management overhead, and streamlined business practices in the Department, with emphasis on the Office of the Secretary of Defense, the Defense Agencies,\textsuperscript{134}


DOD field activities, and the military departments. The task force specifically looked at the private sector and sought to adapt best practices and lessons learned from industry to Pentagon operations. The report recommended reforms in four broad categories:

- Adopting modern business practices to achieve world-class standards of performance. This included moving toward electronic (versus paper) business operations; adopting prime vendor contracting at key facilities for maintenance, repair, and operating materials; consolidating logistics and transportation; reengineering DOD travel procedures and systems; and giving greater options to servicemembers for movement of household goods.

- Streamlining organizations, particularly OSD, the services, and CoCOMs, to remove redundancy and maximize synergy. This included reducing personnel in OSD (reduced by 33% from FY1996 levels), the defense agencies (21% reduction) and field activities (36% reduction), the Joint Staff (29% reduction), the Service Headquarters (10% reduction), and the Combatant Command headquarters (10% reduction). Further actions included
  - Establishing the Defense Threat Reduction and Treaty Compliance Agency to help manage the WMD threat;
  - Establishing a Chancellor for Education and Professional Development;
  - Requiring that the Deputy Director of Military Support for domestic civil emergencies be a General Officer from the National Guard Bureau; and
  - Recommending that OSD policy consolidate from four Assistant Secretary of Defense offices to three.

- Applying market mechanisms to improve quality, reduce costs, and respond to customer needs. This included looking for opportunities to outsource services and functions to the private sector and improve competition for depot maintenance.

- Reducing excess support structures to free resources and focus on core competencies. This included base closures and revitalizing base housing and utilities with private sector capital.

1997—National Defense Panel Report\textsuperscript{134}

Established as an independent panel by the Secretary of Defense under Section 924 of the Military Force Structure Act of 1996, “Transforming Defense: National Security in the 21\textsuperscript{st} Century” provided Congress with an alternative view of the 1997 Quadrennial Defense Review. While it noted that important reforms were ongoing under Secretary of Defense Cohen, the report argued that the pace of DOD transformation should be broader as well as accelerated. Key findings included the following:

- The United States should undertake a broad transformation of its military and national security structures, operational concepts, and equipment, and DOD’s key business processes;

- Transformation should go beyond operational concepts, force structures, and equipment, and should include procurement reform and changes to the support structure, including base closures;

• The concept of “jointness” should be extended beyond the military to the broader national security establishment (a “Goldwater-Nichols for the interagency”);

• The Unified Command Plan should be augmented through:
  • The establishment of an “Americas Command,” to address the challenges of homeland defense as well as those of the Western Hemisphere;
  • The establishment of a Joint Forces Command to be the force provider to the geographic CINCs (later to be called Combatant Commands), address standardization among the various unified commands, oversee joint training and experimentation, and coordinate and integrate activities among the networked service battle labs;
  • Elimination of U.S. Atlantic Command, subordination of Southern Command;
  • Establishment of a Logistics Command that merges necessary support functions divided among various agencies;
  • Assignment of the information domain to Space Command;
  • Initiation of planning and preparedness for urban operations as a matter of priority;
  • Enhanced defense intelligence capabilities, and in particular prioritization of Human Intelligence (HUMINT) collection capabilities;
  • Reconsideration and/or redesign of the PPBS.

2000—The Hart-Rudman Commission

Perhaps picking up from themes touched upon in the 1995 Roles and Missions report and the 1997 National Defense Panel report, the U.S. Commission on National Security in the 21st Century was established in 1998 by Secretary of Defense William Cohen to examine whether U.S. national institutions were appropriately designed to meet the complex challenges of the current and future security environment. It did so in three phases: by first “describing the emerging world in the first quarter of the 21st century, then to design a national security strategy appropriate to that world, and finally to propose necessary changes to the national security structure in order to implement that strategy effectively.” With respect to DOD, the Commission issued a 91-page report outlining key reform proposals, which included

• Restructuring the Office of the Under Secretary of Defense for Policy (USD(P)) by creating a new Assistant Secretary dedicated to Strategy and Planning (S/P) and abolishing the office of the Assistant Secretary for Special Operations and Low-Intensity Conflict;

• Establishing a 10-year goal to reduce infrastructure costs by 20% to 25% through outsourcing and privatizing as many DOD support agencies and activities as possible;

---


Creating a BRAC-like commission on DOD infrastructure reduction that would report to both the legislative and executive branches;

• Moving the QDR to the second year of an Administration, and using the QDR as a foundation for the PPBS process;

• Requiring the Secretary of Defense to produce defense policy and planning guidance that defined specific goals and established relative priorities;

• Requiring those conducting the QDR to aim at defining defense modernization requirements for two distinct planning horizons: near-term (1 to 3 years) and long-term (4 to 15 years);

• Introducing a new process, different from the PPBS, that would require the services to compete for allocation of some resources within the overall DOD budget;

• Revising the Major Force Programs (MFPs) used in the Defense Program Review to focus on a different mix of military capabilities. The 11 MFPs should be expanded into 13 different programs divided into three major categories: combat force programs, combat support programs, and service support programs;

• Updating and modernizing Defense war gaming tools used to assess capabilities and size forces;

• Establishing and employing a two-track acquisition system—one for major acquisitions and a second, “fast track” for a limited number of breakthrough systems, especially those in the area of command and control;

• Returning to the pattern of increased prototyping and the testing of selected weapons and support systems, specifically to foster innovation;

• Implementing two-year defense budgeting solely for the modernization element of the DOD budget (R&D/procurement) because of its long-term character, and expanding the use of multi-year procurement;

• Rewriting the Defense sections of the Federal Acquisition Regulations; and

• Shifting from a threat-based, two major theater war force sizing process to one that measures against recent operational activity trends, actual intelligence estimates of potential adversary’s capabilities, and national security objectives once formulated in the new Administration’s national security strategy.

2001—Quadrennial Defense Review Report\textsuperscript{137}

The 2001 QDR report argued for the recalibration of U.S. strategy to focus on four core goals: assuring allies and friends; dissuading adversaries; deterring aggression and coercion; and defeating enemies. Accordingly, it argued that the Department ought to move from a “threat-based” model to a “capabilities based” model that focused more on how an adversary might fight rather than specifically who the adversary might be or where a war might occur. Still, it retained the essentials of the “two major theater war” construct, noting that “U.S. forces will remain capable of swiftly defeating attacks against U.S. allies and friends in any two theaters of operation in overlapping timeframes,” while also building in the planning requirement to conduct

limited, smaller-scale contingencies. It also sought to better account for risk in defense policy formulation. Other recommendations included the following:

- Maintaining regionally tailored forces forward stationed and deployed in Europe, Northeast Asia, the East Asian littoral, and the Middle East/Southwest Asia to assure allies and friends, counter coercion, and deter aggression;
- Enhancing security cooperation with allies and partners;
- Reorienting the U.S. global military posture to enhance deterrent presence, flexibility, and rapid response in crises;
- Strengthening joint operations through technology;
- Introducing “modularity” to the joint forces;
- Streamlining DOD overhead structure and flattening the organization;
- Consolidating and modernizing defense facility infrastructure; and
- Recalibrating the deploy-to-dwell ratios in order to better control the amount of time DOD personnel are deployed away from home station.

2003—Transformation Planning Guidance

Two years into the Global War on Terror, Secretary of Defense Donald Rumsfeld issued his Transformation Planning Guidance with the goal of transitioning the U.S. military from the industrial age to the information age. As the logic went, particularly after the September 11th attacks, the United States could not afford to react to threats slowly or have large forces tied down for lengthy periods. Rather, the United States needed forces that could take action from a forward position, rapidly reinforce from other areas, and defeat adversaries swiftly and decisively while conducting an active defense of U.S. territory. The roadmap was broken out into eight task categories, to include shaping transformation policy; concept development and experimentation; interoperability; transformation roadmaps; innovative processes; testing; training and education; and measuring progress. It also sought to ensure that transformation activities were included as part of the PPBS cycle.

2004—Joint Defense Capabilities Study

In March 2003, Secretary of Defense Rumsfeld chartered a study—formally named the Joint Defense Capabilities Study—to examine how DOD developed resources and provided joint capabilities. Key findings included the following:

- Services dominate the current requirements process. Much of DOD’s focus is on service programs and platforms rather than capabilities required to accomplish Combatant Command missions;
- Service planning does not consider the full range of solutions available to meet joint warfighting needs; and
- The resourcing function focuses senior leadership effort on fixing problems at the end of the process, rather than being involved early in the planning process.

---

Key recommendations included that

- Joint needs should form the foundation for the defense program;
- Planning for major joint capabilities should be accomplished at the Department rather than the component level;
- Senior leaders should focus on providing guidance and making decisions at the “front end” of the process; and
- A Strategic Planning Council, chaired by the Secretary of Defense, should be established to provide senior leaders with a venue to offer formal inputs to shape defense strategy and support effective oversight of a “capabilities-based” planning system.

On October 31, 2003, Secretary of Defense Rumsfeld issued a memorandum adopting many of these recommendations. These included the planned issuance of a fiscally informed Strategic Planning Guidance document that would replace the policy/strategy sections of the Defense Planning Guidance; the initiation of an enhanced, collaborative joint planning process that articulated metrics for success in the defense program; the planned issuance of fiscally constrained Joint Programming Guidance replacing the programmatic elements of the Defense Planning Guidance; and the issuance of a defense budget informed by all the above activities.

2006—Quadrennial Defense Review

The 2006 QDR process was a key opportunity for DOD to assess the progress it was making, both with respect to the Global War on Terror as well as its implementation of the transformation agenda. Accordingly, it focused on key requirements emerging from operational and defense managerial necessity. Of note, it articulated the need for greater collaboration with other agencies in the national security interagency system to manage a variety of challenges, from counterinsurgency and stability operations to humanitarian assistance and disaster response missions. In its reorientation, it argued for a shift in DOD capabilities from its “traditional” portfolio to one better suited to defeat terrorist networks, prevent acquisition or use of weapons of mass destruction (WMD), defend the homeland in depth, and shape choices of countries at a strategic crossroads. Key reforms contained within the document included the following:

- A Department-wide emphasis on irregular warfare, building partnership capacity, strategic communication, intelligence, and defense institutional reform and governance;
- An increase of Special Operations Forces by 15%;
- Establishment of a Marine Corps Special Operations Command;
- Adoption of a “more transparent, open and agile decision-making process” using common information sources, combining Department-level financial databases, and standardization of analytic processes;
- Establishment of “capital accounts” for major acquisition programs;
- Development of “joint capability portfolios”; and
- Establishment of the Defense Business Systems Management Committee to improve governance of the Department’s transformation efforts.

The 2006 QDR was accompanied by a series of implementation “road maps,” overseen by the Deputy Secretary of Defense.

2010—Quadrennial Defense Review Report

This QDR sought to rebalance the Department and its activities to accomplish the following key priorities: prevail in today’s wars; prevent and deter conflict; prepare to defeat adversaries and succeed in a wide range of contingencies; and preserve and enhance the all-volunteer force. It also paid specific attention to alliance relationships and basing and posture agreements. Key proposed reforms to DOD business practices in the 2010 QDR include the following:

- Reforming security assistance;
- Reforming defense acquisition through a revitalization of the acquisition workforce, bolstering cost analysis, and better integrating risk into cost assessments;
- Institutionalizing rapid acquisition capability; and
- Reforming the U.S. export control system.

2010—Secretary of Defense Gates’s Reforms

During his tenure as Secretary of Defense, Robert Gates sought to recalibrate the Department away from fighting future wars, and instead prioritize fighting and winning the conflicts in which the nation was embroiled at the time, to include Iraq and Afghanistan. He also sought to reduce DOD bureaucracy while at the same time rebuilding the defense civil service. In particular, Secretary Gates

- Disestablished Joint Forces Command; and
- Directed the Department to find $100 billion in overhead savings over five years, and redirect those savings toward personnel and units, force structure, and investment in future capabilities.

In addition, he sought to

- Institutionalize the capabilities necessary to wage asymmetric conflicts;
- “Right-size” the DOD workforce through “in-sourcing”—hiring 13,600 civil servants to replace contractors and hire an additional 33,600 civil servants over five years;
- Reinvigorate the acquisition workforce through adding 4,080 acquisition professionals; and
- Improve medical support during combat operations, for wounded soldiers, and for veterans.

---

143 DOD Comptroller, Budget Justification Briefing, 2010.
2012—Defense Strategic Guidance

On January 5, 2012, Secretary Leon Panetta released strategic guidance intended to articulate priorities for the Department. It argued that four missions would be used to size the force: countering terrorism; deterring and defeating aggression; countering WMD; and homeland defense. It specifically stated that the Department would no longer plan for “large-scale” counterinsurgency or stability operations missions. Key recommendations and decisions taken include

- Managing the force in ways that protect its ability to regenerate capabilities that might be needed to meet future, unforeseen demands;
- Ensuring “reversibility” of decisions—including the vectors on which DOD places its industrial base, so that capabilities that have been divested can be reconstituted if necessary;
- Rebuilding force readiness;
- Reducing defense costs, including growth of manpower costs, and finding efficiencies in headquarters, business practices, and other support activities;
- Examining the mix of Active Component and Reserve Components.

2013—Secretary of Defense Hagel’s Reforms

The Budget Control Act of 2011 eventually resulted in “sequestration,” or mandatory budget reductions for the Department of Defense. This prompted Secretary of Defense Hagel to initiate a “Strategic Choices and Management Review,” which sought to help DOD balance strategic ends, ways, and means under different budget scenarios. It also scrutinized “every aspect” of DOD’s budget, including contingency planning, business practices, force structure, pay and benefits, acquisition practices, and modernization portfolios. Key findings/recommendations included

- Reducing the Department’s major headquarters budgets by 20%, beginning with the Office of the Secretary of Defense, the Joint Staff, Service Headquarters and Secretariats, Combatant Commands, and defense agencies and field activities. Organizations should strive for a goal of 20% reductions in civilian and military personnel on headquarters staffs;
- Reducing the number of direct reports to the Secretary of Defense and eliminating positions; and
- Reducing intelligence analysis and production at Combatant Commands.

2014—Quadrennial Defense Review Report

In part due to fiscal austerity prompted by budget restrictions associated with the Budget Control Act, the 2014 QDR refocused the Department on three strategic objectives: defending the homeland; building security globally by projecting U.S. influence and deterring aggression; and remaining prepared to win decisively against any adversary. This QDR announced force structure

---

reductions, while protecting investments in key capability areas including cybersecurity; missile defense; deterrence; space; air/sea battle; precision strike; intelligence, surveillance and reconnaissance (ISR); counterterrorism; and special operations capabilities. It also sought to rebalance the Department’s “tooth to tail” ratio. The 2014 QDR did not announce many reforms per se; rather, it was focused on recalibrating the defense budget.

Author Contact Information

Kathleen J. McInnis
Analyst in International Security
kmcinnis@crs.loc.gov, 7-1416

Acknowledgments

The author would like to thank Heidi Peters, CRS research librarian, for her contributions to this report.

147 “Tooth to tail” refers to the amount of military personnel (“tail”) it takes to supply and support each combat soldier (“tooth”).
It's time to pump the brakes on Goldwater-Nichols reform. Both House and Senate versions of the FY 2017 National Defense Authorization Act (NDAA) have sections aimed at improving the effectiveness of the Defense Department. And, yes, the intent is laudable. But neither Congress nor the Pentagon has a clear sense of what problem the proposed reforms would solve. Without a clear understanding of the problem, major reforms can end up doing more harm than good.

**What is Goldwater-Nichols?**

The Goldwater–Nichols Department of Defense Reorganization Act of 1986 was a landmark bill that significantly altered the organization and operation of the Department of Defense and its military components. Informed by five years of analysis by Congress and the Pentagon, all the specific provisions of the bill were aimed at
solving one problem (https://www.amazon.com/Victory-Potomac-Goldwater-Nichols-Williams-Ford-
University/dp/1585443980): “the inability of the military services to operate effectively together as a joint team.”
Significantly, the act streamlined the military’s chain of command and required that officers have joint experience
before being promoted into senior positions.

The reform effort arose, in part, as a reaction to two military failures: Operation Eagle Claw and Operation Urgent
Fury. Better known as Desert One, Operation Eagle Claw
(http://www.theatlantic.com/magazine/archive/2006/05/the-desert-one-debacle/304805/) was the 1980 mission
to rescue American hostages in Tehran. Eight service members died and significant equipment was lost, all without
making contact with the enemy. Operation Urgent Fury
(http://www.history.army.mil/html/books/grenada/urgent_fury.pdf) was the U.S. military operation to rescue
Americans in Grenada in 1983. Though the mission largely succeeded, it revealed serious problems — especially in
communications and coordination among the various service components.

Goldwater–Nichols Reform Today

The current debate about the Goldwater–Nichols reform has invoked a wide range of topics — from the Pentagon’s
strategy development process to the department’s organizational structure to the roles and responsibilities of the
National Security Council. But, it has yet to clearly define distinct problems.

Certainly, the debate has not produced clear examples of systemic failure. Though there has been no shortage of
American defense and foreign policy failures over the last decade, it is by no means clear that they have arisen due to
organizational or systemic dysfunction. National security failures in the last decade and a half have largely been the
result of bad decisions and bad leadership — individual problems unlikely to be fixed by systemic change or overhaul.
Bad decision-makers produce bad results, no matter how good the system may be.

While Congress can adjust many of the national security systems and organizations, with the Senate playing a crucial
role in ensuring that qualified people are placed in important positions, Congress cannot guarantee better national
security outcomes simply by mandating processes or organizational designs.

Congressional Action on Goldwater–Nichols

Unfortunately, lack of a clear problem statement isn’t slowing down Congress. Rep. Mac Thornberry (R–Texas)
suggests
that, since threats “have become more trans-regional, multi-domain, and multi-functional, ... [it] compels Congress to
says his reforms are aimed at what he perceives (http://www.brookings.edu/-/media/events/2016/05/19-defense-
authorization/20160519_mccain_defense_transcript.pdf) as a lack of “strategic integration.”

While their analysis of global threats may be correct, the lack of specific examples of U.S. national security failures
makes it hard to determine whether the lack of “strategic integration” is an organizational problem or the result of bad
decisions by senior leaders.

Sen. Tim Kaine (D–Va.), a member of the Senate Armed Services Committee, flagged
(https://www.congress.gov/114/crpt/srpt255/CRPT-114s1.pdf) the lack of clarity this way:
Despite the numerous hearings and countless witnesses, the only theme was that reform was needed with only conceptual suggestions. To date, no study has proposed the legislation contained within this bill. No civilian or military officials offered their views for consideration.

In the absence of a study, independent investigative work or views from outside stakeholders on these provisions due to the embargoed nature of the mark, I am just not sure whether these changes are the right ones or not.

**Congress Should Use the NDAA as a First Step**

Absent a clear problem statement, Congress should exercise caution in proceeding with major structural reforms. All too often, Congress imposes major changes that are either unsuccessful or inflict harm as the result of unintended consequences.

The 2017 NDAA should not be seen as the end-all of Goldwater–Nichols reform but as the foundation upon which substantive reform can be built if needed. For now, Congress should focus on two things:

- **Clearly defining the national security problems that need to be solved.** If the threats today are “trans-regional” and “multi-domain” and the United States struggles with “strategic integration,” the problem may very well sit beyond the walls of the Pentagon. In developing the original Goldwater–Nichols, Congress and the Pentagon took years to hone in on the key problems. Congress and the administration should work together to identify current problems and how to solve them.

- **Strengthening Congress’s ability to affect national security outcomes.** Even if Congress were able to create a better national security infrastructure, bad decision-makers will still produce bad national security outcomes. To guard against bad policy outcomes, Congress should better educate itself on national security issues, including the honest views and security assessments of senior administration officials. Sen. McCain’s proposal in the Senate NDAA ([https://www.congress.gov/bill/114th-congress/senate-bill/2943](https://www.congress.gov/bill/114th-congress/senate-bill/2943)) to replace the Quadrennial Defense Review with an annual presentation of defense strategy could help with that.


Congress can use its tools of oversight, law-making, and funding more aggressively to influence the White House to make the right decisions on national security. A proactive approach is more efficacious than just reacting to bad decisions already in force.

**Conclusion**

The 2017 NDAA offers an opportunity to lay the groundwork for long-term national security reform, but a rush to enact major national security reforms in this bill is misguided. Without a clear definition of the problem, proposed changes may do little or nothing to improve national security. Congress should give national security issues the deliberate analysis they deserve rather than leap to implement remedies that “feel” right. Lawmakers’ first order of business should be to define the problems that need fixing and to strengthen Congress’s own ability to affect national security decisions in the future.

---

Justin T. Johnson is Senior Policy Analyst for Defense Budgeting Policy at The Heritage Foundation. This article is adapted from an original paper ([http://www.heritage.org/research/reports/2016/07/2017-ndaa-define-the-goldwaternichols-problem-before-trying-to-solve-it](http://www.heritage.org/research/reports/2016/07/2017-ndaa-define-the-goldwaternichols-problem-before-trying-to-solve-it)).
WASHINGTON, March 18, 2015 — In a speech to the Brookings Institution's defense fellows here yesterday, the director of the Joint Staff shed light on the process military officials use to provide their best advice to the nation's civilian leaders.

Air Force Lt. Gen. David L. Goldfein said the concept of advising civilian leaders is never far from the minds of the members of the Joint Chiefs of Staff, a group composed of the chairman, the vice chairman, the Army chief of staff, the chief of naval operations, the Air Force chief of staff, the commandant of the Marine Corps and the chief of the National Guard Bureau.

These four-star officers meet in a secure room in the Pentagon called "the tank," Goldfein said. "The chairman is the convening authority," he added, "and he calls the group together to talk about the issues relative to using the military instrument of power."

Painting Provides Reminder of Challenges

The general showed the defense fellows a picture of the only painting that hangs in the tank. Called "The Peacemakers," the 1868 painting by George P.A. Healy shows President Abraham Lincoln meeting with Army Lt. Gen. Ulysses S. Grant, Army Maj. Gen. William T. Sherman and Navy Rear Adm. David Dixon Porter aboard the steamer River Queen in the waning days of the Civil War.

"They were talking about what we now call Phase 4 operations -- post-conflict operations," Goldfein said. "Where I sit in the tank, I stare at this painting, and it's a constant reminder of the gravity and enormity of the challenges we face and the importance of the military advice."

While it is no longer Grant, Sherman and Porter speaking to Lincoln, the process is the same today, the Joint Staff director said, as Army Gen. Martin E. Dempsey, the chairman of the Joint Chiefs of Staff, gives advice to President Barack Obama, Defense Secretary Ash Carter and the other members of the National Security Council.

Goldfein talked about the difference between real and perceived influence and what that means to military advice. Real influence, he said, is established quietly, often behind the scenes, and one relationship at a time. Establishing trust and confidence is essential to being able to have real influence, he explained.

"Perceived influence ... is something that often happens on talk shows. It tends to be very loud," he said. "As a military officer, you have to think about what you are trying to achieve: Is it real influence or is it perceived influence, and where do you want to align yourself?"

Bay of Pigs Proved That Words Matter

Goldfein used the Bay of Pigs fiasco in 1961 to illustrate the point "that words matter." Although it was a CIA operation to depose Cuba's Fidel Castro, he said, the plan had a military aspect, and the Joint Chiefs of Staff examined it and concluded that it had a 30 percent chance of success. Somehow, the general said, that got communicated to the newly inaugurated President John F. Kennedy that there was "a fair chance of success."

The operation failed, and Kennedy believed the Joint Chiefs did not give him the candid military advice a president expects and deserves. Goldfein showed a picture of the Joint Chiefs meeting with Kennedy in the White House Cabinet Room a month after the operation.

In giving best military advice, leaders must be aware there are two ways of looking at the world today, Goldfein said. "I call it the 'fear' and 'fear not' perspectives," he told the defense fellows.

On one side is the fear perspective, he said, fueled by issues that crop up around the world that have a military aspect, such as the rise of the Islamic State of Iraq and the Levant and Russia taking Crimea and threatening Eastern Ukraine. He also cited problems with Boko Haram in Africa and terror groups in Libya, Syria, Afghanistan, Pakistan, Somalia and Yemen. In addition, the general noted the Ebola epidemic in West Africa.
Joint Staff Director Describes Military Advice Process > U.S. DEPARTMENT OF DEFENSE > Article

Last year was the most complex year since 1960, the general said. Another way of looking at it, he said, is to say that there is no existential threat to the United States. Last year continued an overall drop in violence around the world, he noted, and more people in more places are prosperous. This is the “fear not” version of the world, he said, and a case can be made that both perspectives are right.

Different Perspectives Affect the Process

The different perspectives that military leaders and civilian leaders have also play a role in the process of military leaders providing advice, Goldfein said. As a military leader, he added, he wants civilian leaders to tell him the strategic objective of what they are trying to accomplish.

But civilian leaders want options, he said. “So we want objectives, they want options,” he told the defense fellows. “They ask us for options, and we ask them ‘What’s your objective?’”

Having those two ways of coming at the same problem works, he said, but both sides need to understand the differences.

(Follow Jim Garamone on Twitter: @garamoneDoDNews)

---

Related Biographies


Related Sites

Joint Chiefs of Staff (http://www.jcs.mil/)
The Defense Department on Facebook (https://www.facebook.com/deptofdefense)
The Defense Department on Twitter (https://twitter.com/deptofdefense)
DoD News on Twitter (https://twitter.com/dodnews)
DoDLive Blog (http://www.dodlive.mil/)
DoD News Broadcast Channel (http://dodnews.defense.gov/)

---

News
Secretary of Defense
Deputy Secretary of Defense
Photos/Videos
Other

---

Recent News Articles

10/17/2016

10/17/2016
DoD Recognizes Innovative Initiatives to Prevent Sexual Assault (http://www.defense.gov/News/Article/Article/975474/doD-recognizes-innovative-initiatives-to-prevent-sexual-assault)

10/17/2016
Iraqi Forces Begin Battle for Mosul (http://www.defense.gov/News/Article/Article/975239/iraqi-forces-begin-battle-for-mosul)

10/16/2016

10/15/2016

http://www.defense.gov/News/Article/Article/604295
10 U.S. Code § 151 - Joint Chiefs of Staff: composition; functions

Current through Pub. L. 114-38. (See Public Laws for the current Congress.)

(a) Composition.—There are in the Department of Defense the Joint Chiefs of Staff, headed by the Chairman of the Joint Chiefs of Staff. The Joint Chiefs of Staff consist of the following:

(1) The Chairman.

(2) The Vice Chairman.

(3) The Chief of Staff of the Army.

(4) The Chief of Naval Operations.

(5) The Chief of Staff of the Air Force.

(6) The Commandant of the Marine Corps.

(7) The Chief of the National Guard Bureau.

(b) Function as Military Advisers.—

(1) The Chairman of the Joint Chiefs of Staff is the principal military adviser to the President, the National Security Council, the Homeland Security Council, and the Secretary of Defense.

(2) The other members of the Joint Chiefs of Staff are military advisers to the President, the National Security Council, the Homeland Security Council, and the Secretary of Defense as specified in subsections (d) and (e).

(c) Consultation by Chairman.—

(1) In carrying out his functions, duties, and responsibilities, the Chairman shall, as he considers appropriate, consult with and seek the advice of—

(A) the other members of the Joint Chiefs of Staff; and
(B) the commanders of the unified and specified combatant commands.

(2) Subject to subsection (d), in presenting advice with respect to any matter to the President, the National Security Council, the Homeland Security Council, or the Secretary of Defense, the Chairman shall, as he considers appropriate, inform the President, the National Security Council, the Homeland Security Council, or the Secretary of Defense, as the case may be, of the range of military advice and opinion with respect to that matter.

(d) Advice and Opinions of Members Other Than Chairman.—

(1) A member of the Joint Chiefs of Staff (other than the Chairman) may submit to the Chairman advice or an opinion in disagreement with, or advice or an opinion in addition to, the advice presented by the Chairman to the President, the National Security Council, the Homeland Security Council, or the Secretary of Defense. If a member submits such advice or opinion, the Chairman shall present the advice or opinion of such member at the same time he presents his own advice to the President, the National Security Council, the Homeland Security Council, or the Secretary of Defense, as the case may be.

(2) The Chairman shall establish procedures to ensure that the presentation of his own advice to the President, the National Security Council, the Homeland Security Council, or the Secretary of Defense is not unduly delayed by reason of the submission of the individual advice or opinion of another member of the Joint Chiefs of Staff.

(e) Advice on Request.—

The members of the Joint Chiefs of Staff, individually or collectively, in their capacity as military advisers, shall provide advice to the President, the National Security Council, the Homeland Security Council, or the Secretary of Defense on a particular matter when the President, the National Security Council, the Homeland Security Council, or the Secretary requests such advice.

(f) Recommendations to Congress.—

After first informing the Secretary of Defense, a member of the Joint Chiefs of Staff may make such recommendations to Congress relating to the Department of Defense as he considers appropriate.

(g) Meetings of JCS.—

(1) The Chairman shall convene regular meetings of the Joint Chiefs of Staff.

(2) Subject to the authority, direction, and control of the President and the Secretary of Defense, the Chairman shall—

(A) preside over the Joint Chiefs of Staff;

(B) provide agenda for the meetings of the Joint Chiefs of Staff (including, as the Chairman considers appropriate, any subject for the agenda recommended by any other member of the Joint Chiefs of Staff);

(C) assist the Joint Chiefs of Staff in carrying on their business as promptly as practicable; and

(D) determine when issues under consideration by the Joint Chiefs of Staff shall be decided.

LII has no control over and does not endorse any external Internet site that contains links to or references LII.

U.S. Code Toolbox


Law about... Articles from Wex (/wex/wex_articles)
Title 10 USC, RSS Feed 📥 (https://www.law.cornell.edu/uscode/rss/usc_update_10.rss)
Table of Popular Names (/ttopn)
Parallel Table of Authorities (/ptoa)

Find a Lawyer

About LII
PANEL III:

CYBER CHALLENGES FOR THE NEW ADMINISTRATION

MODERATOR:

MAJ. GEN. CHARLES DUNLAP JR., USAF (RET.)
Why is the President downplaying alleged Russian attempts to influence U.S. elections? Maybe he doesn’t oppose all efforts to impact foreign voters

BY CHARLIE DUNLAP, J.D. · 19 SEPTEMBER 2016

Last week ABC News ran a story “Russian Hacking: Why the U.S. Isn’t Retaliating” which sought to explain why, “after weeks of news stories describing Russian intelligence operations to hack into the U.S. political system,” current and former U.S. national security officials are nevertheless saying (surprisingly to me) that “[n]ot very much” will be done about it by the U.S., “at least in the near term.”

Why? ABC reports:

Among the reasons: officials don’t want to reveal intelligence sources and methods that provide them insight into the activities Russian cyber spies; the U.S. is seeking Russian cooperation in Syria; and American officials worry that an escalating cyber tit for tat between the two powers could hurt U.S. interests more than it helps.

Earlier in September, the President “acknowledged that the Russians have been attacking U.S. institutions on the internet” but also said that:

“Our goal is not to suddenly in the cyber arena duplicate a cycle of escalation that we saw when it comes to other arms races in the past, but rather to start instituting some norms so that everybody’s acting responsibly,” Mr. Obama said. “What we cannot do is have a situation in which suddenly this becomes the wild, wild West, where countries that have significant cybercapacity start engaging in unhealthy competition or conflict through these means.”

Still, it does seem rather curious that the President seems to think that inaction on the U.S.’s part will somehow discourage Russia (or any foreign government) from attempting to influence U.S. voters, via cyber means or otherwise. In fact, an argument can be made that the failure to respond will only encourage more machinations by Russia or whoever is behind the efforts.

But the President may have another, subtler reason in mind for downplaying the reported Russian activities: he simply doesn’t want an international norm to develop which would condemn a nation for attempting to influence a foreign election. After all, he’s done it himself.
Last April *The Guardian* reported that during the President's trip to the U.K., he weighed in with British voters about the then-pending issue of whether or not Britain would leave the European Union (Brexit):

Barack Obama has warned that the UK would be at the "back of the queue" in any trade deal with the US if the country chose to leave the EU, as he made an emotional plea to Britons to vote for staying in.

And the President is hardly alone in trying to affect another country's electorate. The *Washington Post* reports that 61 foreign leaders have publicly criticized Donald Trump. Perhaps of more interest is Hillary Clinton's claim that foreign leaders had reached out to her *privately* about helping her defeat Trump (and, except for Italy's Prime Minister Matteo Renzi, she has declined to reveal which foreign leaders are involved).

Are we collectively schizophrenic about this issue? At last summer's *Aspen Security Forum* there was much discussion about the hack of the Democratic National Committee (DNC) email system as an example of a disgraceful effort by a foreign government to influence the U.S. election. According to the *New York Times*, the material revealed:

Top officials at the Democratic National Committee criticized and mocked Senator Bernie Sanders of Vermont during the primary campaign, even though the organization publicly insisted that it was neutral in the race…

In addition, the *Washington Post* said, "[l]nternal Democratic National Committee emails appear to show officials discussing using Sen. Bernie Sanders's faith against him with voters."

For me, the complicating part of this is that the information revealed was apparently accurate, and that factor raises questions such as these: irrespective of the source, to what extent was this the kind of information voters ought to have? Should voters be informed, for example, about a nefarious idea to use a candidate's faith against him?

In short, is releasing *accurate* information a proper and even honorable way to attempt to influence an election in another country? (Espionage, incidentally, typically violates the victim's national law, but is not generally prohibited by international law.)

Exactly how far a nation ought to go in attempting to influence foreign voters caused me to pose this question to Representative Adam Schiff (D-CA), the Ranking Member, House Permanent Select Committee on Intelligence, at *Aspen*:

[I]f it is wrong to try to influence voting in another country, was President Obama wrong when he came out against the Brexit vote and warned about impact on trade and so forth prior to that vote?

After responding that he wasn’t sure that the President’s effort with respect to the Brexit was strategically effective, he said this:

But it’s a quite a different story to publicly express an opinion and privately, surreptitiously hack in and try to influence an election by disclosing private emails. So I wouldn’t put those in the same category at all.
I followed up with this question in reference to *surreptitiously* trying to influence a foreign election: “Would we ever do it?” Here’s his interesting response:

MR. SCHIFF: Well, the question would we ever do it. You know, there certainly have been many documented instances in the past where the IC [intelligence community] has attempted to influence political processes elsewhere. I can’t go into any kind of a covert action question here obviously.

In my view, any effort by a foreign government to actually manipulate election results in the U.S. by, for example, hacking into voting machines to change votes, is extraordinarily threatening to our way of life and needs to be addressed accordingly. However, imposing electoral transparency by disclosing *accurate* information seems to me to be something different.

Accordingly, let’s ask ourselves this: if the U.S. could influence an election in a hostile country *not* by manipulating voting machines or even by covertly distributing *disinformation*, but rather by openly (or covertly) releasing *accurate* material – however obtained – *should* the U.S. do it?

Representative Schiff isn’t saying, and the President has passed on the opportunity to make a strong statement in opposition. Is there a message there?
Can litigation against social media platforms help disarm terrorist organizations?

BY CHARLIE DUNLAP, J.D.  22 AUGUST 2016

I have long believed that it is a melancholy but inescapable truth that in too many cases it takes litigation to get powerful corporate interests to do what they ought to do in the public interest. These days I think that there are instances where civil or criminal legal action against social media companies whose platforms are being used by terrorists could provide a needed incentive.

It’s no secret to the companies that their social media platforms have become key enablers of terrorism. CIA Director John Brennan called them out when he told Congress last June that:

ISIL (Islamic State of Iraq and the Levant) releases a multitude of media products on a variety of platforms—including social media, mobile applications, radio, and hardcopy mediums. To disseminate its official online propaganda, the group primarily uses Twitter, Telegram, and Tumblr, and it relies on a global network of sympathizers to further spread its messages.

It’s undeniable that we live in an age—as researchers at the Danish Defence College put it—of the “weaponization of social media,” and that our terrorist enemies are very successfully using that “weapon.”

What to do about it? Over on Lawfire I discuss (“Do Both Candidates Support More Aggressive Material Support Litigation?”) using civil and criminal processes against social media platforms where their products are proven to be providing “material support” to terrorists and/or terrorist organizations.

It is true that in the shadow of burgeoning civil litigation some social media companies have begun to take down thousands of accounts connected with terrorism that violate their user agreements. But I also believe that more can be done, and that seismic change in industries can be spurred by litigation as there is nothing like the specter of jail or enormous civil judgments to motivate them to reform themselves.

Ask yourself: without litigation would the auto industry have built safer cars? Would big tobacco have put prominent warnings on their products? Would the pharmaceutical companies have worked as hard as they do to ensure the safety of their drugs? And more recently, do you think that the Arab Bank case just might cause financial institutions to be more wary of their shady customers?

Anyway, again, the longer discussion is found here.
Have government lawyers “winced” at “cyber bomb” statements? If so, it may be about norm development

BY CHARLIE DUNLAP, J.D. · 9 MAY 2016

Is there anything legally problematic about government officials equating cyber operations as being “just like” dropping “bombs”? Before getting to that, let’s consider a little context.

In recounting progress in the campaign against the Islamic State of Iraq and the Levant (ISIL) the President announced in mid-April that “cyber operations are disrupting their command-and-control and communications.” This followed Feb. 29th news conference statements along the same lines by Secretary of Defense Ashton B. Carter (and echoed by Chairman of the Joint Chiefs of Staff General Joseph F. Dunford).

Carter said that the U.S. was “using cyber tools to disrupt ISIL’s ability to operate and communicate over the virtual battlefield.” In response to a follow-up question he added:

With respect to cyber, I think you’re referring to our use of cyber which we have talked about generally. In the counter-ISIL campaign in — particularly in Syria to interrupt, disrupt ISIL’s command and control, to cause them to lose confidence in their networks, to overload their network so that they can’t function, and do all of these things that will interrupt their ability to command and control forces there, control the population and the economy.

Here’s something else from that news conference to keep in mind as we examine this issue: Carter also said: “because the methods we’re using are new, some of them will be surprising and some of them are applicable to other challenges that I described, other than ISIL, that we have around the world.” (Italics added.)

To me it’s obvious that the U.S. wants the world to know (likely as a means of enhancing deterrence) that it has offensive cyber capabilities, and is willing to use them. This also appears to be part of an orchestrated effort by the U.S. to take the lead in developing internationally accepted norms as to the use of cyber methodologies in armed conflict (something I support).

Doing so would be a logical follow-on to the inclusion in the 2015 Department of Defense Law of War Manual of a chapter on cyber operations. In many respects, this is a very important policy initiative that would have been unheard of even just a few years ago, and one that could be seen as answering critics concerned about paucity (until recently) of expressions of official views of the U.S. and other countries. Indeed, the New York Times pointed out in an April 24th article that “[a]s recently as four years ago, [the Pentagon] would not publicly admit to developing offensive cyberweapons or confirm its role in any attacks on computer networks.”
The U.S.’s new openness and assertiveness about cyber operations is particularly meaningful because the views of the U.S. – as a “specially affected State” vis-à-vis cyber – would be quite influential in developing norms as to how international law assesses cyber activities in wartime. But what kinds of cyber activities are we talking about?

Besides what Secretary Carter relayed, the Times claims that “interviews with more than a half-dozen senior and midlevel officials” indicated that “the plan is to imitate [ISIL commanders] or to alter their messages, with the aim of redirecting militants to areas more vulnerable to attack by American drones or local ground forces.” According to the Times, officials also said that the U.S. may use “cyberattacks to interrupt electronic transfers and misdirect payments” involving ISIL.

Nevertheless, some consternation apparently arose when the Deputy Secretary of Defense Robert O. Work mentioned that “[w]e are dropping cyberbombs” on ISIL. The Times said “some of Mr. Work’s colleagues acknowledged that they had winced when he used the term, because government lawyers have gone to extraordinary lengths to narrowly limit cyberattacks to highly precise operations with as little collateral damage as possible.” Actually, Mr. Work was only reiterating what his boss, Secretary Carter, had told NPR on February 28th:

I’m talking about attacking the ability of someone sitting in Raqqa to command and control ISIL forces outside of Raqqa or to talk to Mosul or even to talk to somebody in Paris or to the United States. So these are strikes that are conducted in the war zone using cyber essentially as a weapon of war. Just like we drop bombs, we’re dropping cyber bombs. (Italics added.)

In any event, the Times’ explanation of the ‘wincing’ is a bit puzzling to me because in an era of precision-guided munitions equating a cyber-operation to a “bomb” does not, ipso facto, suggest imprecision or extensive collateral damage. But saying that cyber operations are “just like” dropping “bombs” does imply significant physical effects, and that is – legally speaking – rather important.

Specifically, much more than de minimis permanent physical damage caused by a cyber-technique could result in its employment being characterized as a use of force under international law, and that carries a number of legal implications far more consequential than one that isn’t considered as rising to that level. Yet determining exactly what constitutes “force” in the cyber realm has been tricky and controversial. Here’s how the DoD Law of War Manual explains it:

Article 2(4) of the Charter of the United Nations states that “[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

Cyber operations may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law. For example, if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under jus ad bellum, then such cyber operations would likely also be regarded as a use of force. Such operations may include cyber operations that: (1) trigger a nuclear plant meltdown; (2) open a dam above a populated area, causing destruction; or (3) disable air traffic control services, resulting in airplane crashes. Similarly, cyber operations that cripple a military’s logistics systems, and thus its ability to conduct and sustain military operations, might also be considered a use of force under jus ad bellum. (Bolding added.)

What all this could mean is that “government lawyers” are concerned about establishing an international norm that equates the cyber operations now being employed against ISIL as a “use of force.” In other words, if those cyber operations really are “just like” dropping “bombs” it conjures up notions of effects.
much the same as those “caused by traditional physical means” as the Law of War Manual puts it, and that is “force” within the meaning of international law.

Why would this be important? Though the U.S. is already engaged in a lawful armed conflict against ISIL, that may not necessarily the case with the “other challenges” beyond ISIL to which Carter suggested the same cyber methods may be “applicable.”

If those “challenges” (and especially those that are nation-states) who are on the receiving end of the same cyber methods the U.S. may be using against ISIL, consider the operations as being “just like” having “bombs” dropped on them, that could provide legal support for a response of a kind that the U.S. does not intend to trigger.

Here’s why: when the Law of War Manual talks about cyber operations that are “considered a use of force under jus ad bellum,” it is referencing the kind of scale and intensity of force that would permit a nation to respond in self-defense. Consider that Article 51 of the UN Charter explicitly preserves the “inherent right of individual or collective self-defense if an armed attack occurs against a member State. (The U.S. considers “force” as used in Article 2 (4) as conterminous with “armed attack” as used in Article 51 – see paragraph 16.3.3.1 of the Law of War Manual.)

Put another way, despite the “cyber bomb” statements of the DoD officials, the U.S. may yet want international norms to consider the techniques being used against ISIL, though harmful to them, as still being below the threshold of the legal interpretation of “force” as found in Article 2(4) of the UN Charter or “armed attack” as used in Article 51. This is especially so if the “challenges” that it has “around the world” are entities with which the U.S. is not currently engaged in an armed conflict against, and with whom it does not wish to start one.

For example, it’s possible that the U.S. government lawyers don’t want a norm to develop that would hold that a cyber-method that only produces a temporary disruption of communications (and which doesn’t produce any lasting physical damage) to be “just like” dropping a traditional “bomb.”

In fact, it may well be in the U.S. interest to have available an array of cyber methodologies (to include some or all those being used against ISIL) that can create effects on opponents advantageous to the U.S. yet do not breach the UN Charter because they would not, from a legal perspective, amount to a use of “force.” Of course, we need to remember that below the threshold of force cyber operations can be unfriendly and harmful in a non-kinetic sense, and thus carry their own legal complexities (which will be addressed by the forthcoming Tallinn 2.0 Manual).

Still, I think it’s important for the U.S. to avoid appearing to characterize its cyber activities as uses of “force” if it’s not really necessary to do so. Accordingly, it needs to be careful about what messages it might unintentionally send to the international community as to what is – or is not – “just like” dropping “bombs.”
There is no universally agreed definition [for sovereignty], but considerations of international sovereignty revolve around the recognition of a government's right to exercise exclusive control over territory, and this definition is ill suited for cyber discussions. For convenience we might refer to "the geography of cyberspace," but I challenge you to point to cyberspace. Although cyberspace is all around us, when trying to point at it you will be as unable to as the Square in [Edwin] Abbott's Flatland was to point to "up." I always found it troubling to hear military commanders talk in terms of seizing the cyber "high ground" or negotiating "cyber terrain." That was language they were comfortable with, but in any meaningful sense of the word, cyber lacks geography.
Recent years are full of reports of cyber incidents in which, from time to time, significant damage is done by way of a cyber operation. Examples include the 2007 cyber assault on Estonia by pro-Russian "hacktivists" that temporarily shut down many governmental and private sector operations, the 2012 "Shamoon" virus that damaged 30,000 computers at Saudi Arabia's Aramco and was claimed by the "Cutting Sword of Justice," the 2013 cyber shutdown of the New York Times by the Syrian Electronic Army, and of course the infamous Stuxnet malware that damaged almost one thousand centrifuges at an Iranian nuclear facility and has been attributed to the United States and Israel by many cyber experts.

*277 Each of these cyber events, and the multitude of others that have occurred and continue to occur daily, raises important questions about the role and responsibility of States with respect to cyber incidents. Do States exercise sovereign control over the cyber infrastructure that sits on their territory? If so, do States have a responsibility to control the cyber activities that emanate from or even just pass through their sovereign cyber assets? In other words, to what extent does a State have to control activities of non-State actors, such as private hacktivists, criminal organizations, and terrorists, when those cyber actions may cause harm to others?

The answer to these questions revolves in large part around the international law doctrine of sovereignty. The extent to which nations exercise sovereignty over cyberspace and cyber infrastructure will provide key answers to how much control States must exercise and how much responsibility States must accept for harmful cyber activities when they fail to adequately do so.

This Article argues that States have sovereign power over their cyber infrastructure and that with that sovereign power comes corresponding responsibility to control that infrastructure and prevent it from being knowingly used to harm other States. This responsibility to prevent external harm extends not *278 only to State actors, but also to non-State actors. This sovereign power and responsibility, while almost exclusive, necessarily has some limitation.

The Introduction to this Article will introduce the underlying assumptions of sovereignty and set the stage for a review of some of the cardinal principles of sovereignty and their application to cyberspace in light of each State's corresponding sovereign duties and obligations. Parts I and II will then look at the fundamental principles of sovereignty, consider how these principles apply to cyber activities and what corresponding cyber duties and obligations those principles implicate, and then consider related issues that naturally arise from that application.

INTRODUCTION

In the emerging area of cyber operations, the application of the doctrine of sovereignty to cyber activities has created an ongoing debate among States, academics, and practitioners. The recently published Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) reflects some of this controversy in its short section on sovereignty.

Current State practice suggests that States are hesitant to accept responsibility for cyber activities that come from within their sovereign territory. In none of the examples discussed in the Preface did any State accept responsibility for the cyber actions that occurred. In fact, the opposite is true. In the case of the cyber assaults on Estonia, Russia not only disclaimed any responsibility, but has proven unresponsive to requests by Estonia for investigation and extradition of the potential offenders who acted from within Russian territory. In the case of the Stuxnet malware, despite numerous allegations that the United States and Israel were involved, neither country has officially admitted responsibility.

This hesitation on the part of States to accept responsibility for incidents that occur over the Internet is the product of two major issues inherent in the structure of the Internet: the difficulty of timely attributing an attack and the random method in which data travels over the Internet infrastructure, normally taking the path of least resistance without respect to geography. 16

The issue of cyber attribution has been well documented 17 and needs only brief comment here. The nature of the Internet allows anonymity, including for those who desire to represent themselves to be someone else. This anonymity acts as “an open invitation to those who would like to do [] harm, whatever their motives.” 18 This inherent difficulty in timely attribution makes States wary of accepting responsibility for attacks from within their territory because not only can they not always identify the attacker in a timely manner, but because even if they can identify the computer from which the cyber act originates, they are unlikely to know who is behind the computer. 19

Similarly, anonymity allows States to take actions, knowing that timely attribution is impossible. 20 This is especially true of actions taken by States through proxies, such as non-State actors. 21

Additionally, the nature of data flow on the Internet makes States hesitant to accept responsibility for cyber activities that flow from within their territory. Cyber data, by its nature, seeks out the path of least resistance over the available cyber infrastructure. 22 In other words, an email sent from a computer in one city to a recipient in that same city may travel through any number of foreign countries before arriving at its destination. 23 The same is true of cyber malware. And this data is not only uncontrollable by the sender in how it travels, but also largely uncontrollable by the States through which the data passes. This means that malware may traverse any number of States before reaching the target State. Transit States do not want to be responsible for the harmful data in these types of scenarios.

Despite the hesitance of States to accept responsibility for attacks crossing their cyber infrastructure, there is a fundamental assumption in international law that authority and obligations strive to stay in balance with each other. 24 In other words, when the international paradigm allocates authority to a State, it almost always allocates a corresponding responsibility or obligation. 25 The application of this principle was illustrated as far back in history as the legitimization of the Westphalian system. When States became the primary actors in the international community, they did so with the understanding that they would possess a monopoly on force within their geographic borders. 26 In correspondence to that obligation came the grant of authority for sovereigns to raise armies and navies that would be reciprocally recognized by other States and given combatant immunity in any future conflicts, as long as those armies and navies acted in accordance with the sovereign's wishes and the provisions of any international agreements to which the sovereign had acceded. 27

The practical application of this balance is seen in the Instruction for the Government of Armies of the United States in the Field, 28 known as the Lieber 281 Code. 29 This Code was written by Francis Lieber and issued by President Abraham Lincoln to provide guidance to the Union armies during the American Civil War. 30 Article 57 of the Lieber Code proclaims, “So soon as a man is armed by a sovereign government and takes the soldier's oath of fidelity, he is a belligerent; his killing, wounding, or other warlike acts are not individual crimes or offenses.” 31 In other words, once the sovereign was exercising the responsibility to monopolize and control violence through its agents, those agents were granted authority to use force on behalf of the sovereign with immunity, even when fighting against other sovereigns. 32

This balance between responsibility and authority continues to underlie the modern law of armed conflict. The laws with respect to prisoners of war, 33 the treatment of civilians during armed conflict, 34 and targeting 35 all reflect the balanced grant of authority and obligation. The balance also applies directly to the principle of sovereignty. As stated
in the International Court of Justice's (ICJ) *Corfu Channel* case, "Sovereignty confers rights upon States and imposes obligations on them." 36

As a starting point, it is important to note that international law must also be considered to apply to cyberspace and cyber technologies. As stated in the United States' 2011 International Strategy for Cyberspace, "The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior -- in times of peace and conflict -- also apply in cyberspace." 37

*282* It follows, then, that the international law doctrines applying to sovereignty would apply to cyber technologies. Where international law grants authority for States with respect to cyberspace and the application of cyber technologies, it also imposes duties and obligations. As nations exercise sovereign power over aspects of cyberspace, or exert sovereign authority over cyber infrastructure, they must necessarily accept the corresponding obligations and duties that come with that assertion of authority.

The following Parts of this Article will review some of the cardinal principles of sovereignty and their application to cyberspace and then consider the corresponding duties and obligations. In each case, the principle of sovereignty will be stated and defined. Its application to cyberspace will then be discussed, including the corresponding duty or obligation that arises from that assertion of sovereignty. An example of the duty and obligation will be used to help clarify the analysis. Finally, issues that arise from the assertion of that authority and its corresponding duty or obligation will be highlighted.

I. STATES ARE SOVEREIGN AND EQUAL

When the nation-State emerged in seventeenth-century Europe, it brought with it the doctrine that the international community would consist of geographically organized and controlled entities that would have at least two characteristics. First, those entities would be sovereign, and second, they would be equal, regardless of size or composition. 38 These two characteristics of States remain in force today and have significant impacts on cyberspace and cyber operations.

A. Sovereignty

Sovereignty is inherent to statehood and, in fact, is often termed the "basic constitutional doctrine of the law of nations." 39 The meaning of the term "sovereignty" has been a point of discussion for centuries 40 and remains so today. 41 However, it is manifested in certain rights and corresponding obligations. A basic review of those rights and obligations will assist in discerning the impact of sovereignty on cyber operations.

*283* 1. Rights

Sovereignty confers rights on two distinct planes or spheres: the domestic sphere and the international sphere. In other words, sovereignty is understood to be "the collection of rights held by a State, first in its capacity as the entity entitled to exercise control over its territory and second in its capacity to act on the international plane, representing that territory and its people." 42

With respect to the domestic sphere, sovereignty provides exclusivity in power and authority. This was confirmed in the *Island of Palmas* Arbitral Award of 1928. 43 The arbitral decision provides that "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the
exclusion of any other State, the functions of a State.\textsuperscript{44} One of the most fundamental rights of sovereignty, then, is exclusivity of power within the sovereign's own territory, particularly as opposed to the exercise of rights in that territory by some other sovereign.\textsuperscript{45}

The ICJ in its \textit{Corfu Channel} decision confirmed this understanding of sovereignty. "By sovereignty [sic], we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States."\textsuperscript{46}

Though a State's sovereign power is nearly absolute, it is limited by certain international law principles,\textsuperscript{47} including actions of the U.N. Security Council,\textsuperscript{48} the law of armed conflict,\textsuperscript{49} and fundamental human rights.\textsuperscript{50} There are also areas where, based on consensual agreement and custom, no State can assert sovereignty, such as the high seas.\textsuperscript{51} This area has been treated as \textit{res communis}, meaning that it \textsuperscript{*284} belongs to all States and can be appropriated by no State.\textsuperscript{52} There are other areas where actors have agreed to non-exclusive sovereignty such as Antarctica,\textsuperscript{53} the seabed,\textsuperscript{54} and the moon.\textsuperscript{55} These are areas where no sovereign exercises power, but where all sovereigns share power, based on agreement.

2. Obligations

As discussed above, international law tries to keep in balance rights and obligations. This is reflected in the ICJ's statement, "Sovereignty confers rights upon States and imposes obligations on them."\textsuperscript{56} Therefore, in correspondence with the rights and authorities discussed above, the principle of sovereignty also imposes obligations which deserve discussion here.

Obligations tied to sovereignty include the obligation to recognize the sovereignty of other States,\textsuperscript{57} the obligation of non-intervention into the areas of exclusive jurisdiction of another State,\textsuperscript{58} and the obligation to control the actions that occur within the sovereign's geographic boundaries.\textsuperscript{59}

The obligation to recognize the sovereignty of other States is simply the obverse of the right of a State to exercise its own sovereignty. In claiming the rights that come with sovereignty, there is an implicit recognition of the right of others to make similar claims and exercise similar rights.

Once another State has made such claims, and those claims are recognized, other sovereigns have a legal obligation to not interfere with the sovereign rights of the other State. Though there are legitimate exceptions to this rule,\textsuperscript{60} the obligation of non-intervention is well recognized in international law.\textsuperscript{61}

\textsuperscript{*285} Another obligation that grows out of sovereignty is the requirement to control actions from within a State's sovereign control from having deleterious effects on others.\textsuperscript{62} This obligation is worth mentioning here but will be discussed further below.

\textbf{B. Equality}

The principle of the sovereign equality of States laid out in Article 2.1 of the U.N. Charter States: "The Organization is based on the principle of the sovereign equality of all its Members."\textsuperscript{63} This principle of equality is based on the historical maxim "\textit{par in parem non habet imperium}," or "an equal has no power over an equal,"\textsuperscript{64} which is considered by some
to be the first, and perhaps most fundamental, principle of sovereignty.\textsuperscript{65} As such, certain rights and obligations accrue from this accepted equality.

1. Rights

As equals under international law, States have the right to deal with each other on equal footing, with equal consideration under the law. "If states (and only states) are conceived of as sovereign, then in this respect at least they are equal, and their sovereignty is in a major aspect a relation to other states (and to organizations of states) defined by law."\textsuperscript{66} While skeptics argue that the practical reality of this is far from being true, with large and powerful States clearly exerting unequal pressures on smaller and weaker States to bow to their desires,\textsuperscript{67} equality is still guaranteed under the law. Regardless of what some identify as the reality of international politics where "while all States are equal, some are more equal than others,"\textsuperscript{68} the legal regime is established with a clear preference to equality and maintenance of the status quo. "The United Nations are [sic] based on the principle of sovereign equality of all its members and preserving state sovereignty is a top priority for both international organizations and individual States."\textsuperscript{69}

\*286 Some of the obvious rights that accrue from international equality include an equal right to global commons,\textsuperscript{70} the right to develop and utilize domestic resources without non-consensual external constraints,\textsuperscript{71} and the right to discourse on the international scene as an equal. These rights are also tempered with corresponding obligations.

2. Obligations

Several obligations flow from the principle of sovereign equality. First, States must act with due regard for the rights of other sovereigns.\textsuperscript{72} There is some discussion as to how far-reaching this obligation of due regard is, but it is at least applicable by treaty to the global commons,\textsuperscript{73} natural resources,\textsuperscript{74} the environment,\textsuperscript{75} and during times of armed conflict.\textsuperscript{76}

The obligation of due regard, though not clearly defined in international law, is generally thought of as an obligation to ensure that the exercise of one State's rights does not cause undue harm to another State's exercise of its rights.\textsuperscript{77} It is \*287 understood to have two components: 1) an "awareness and consideration of either State interest(s) or other factor(s)," and 2) a balancing of those interests and factors when making a decision.\textsuperscript{78}

Another obligation that has its foundation in sovereign equality is the obligation to solve disputes peacefully. This obligation is clearly stated in the U.N. Charter\textsuperscript{79} and has been stated in General Assembly statements and resolutions,\textsuperscript{80} applied in decisions of the ICJ,\textsuperscript{81} and has been duplicated in bilateral and multilateral treaties.\textsuperscript{82}

While there is no obligation to solve all disputes, States are obligated to resolve disputes peacefully if they have the potential to endanger the maintenance of international peace or security.\textsuperscript{83} Additionally, if States elect to resolve disputes that do not endanger international peace and security, they must also resolve these disputes peacefully, though there is no legal obligation to resolve these disputes at all.\textsuperscript{84}

\textit{C. Application to Cyberspace}

As stated above, the doctrine of sovereignty and the principles it espouses have direct application to cyberspace. As States exercise their sovereign rights, they can do so in cyberspace but must also accept the corresponding obligations that
apply. The next two Subparts will consider the principles of sovereignty and equality and apply the rights and obligations discussed above to cyberspace, as well as identify some lingering issues that will need further resolution.

1. Sovereignty

As a matter of sovereignty, States have the right to develop their cyber capabilities according to their own desires and resources. A State may choose to extensively develop its cyber capabilities and make them available broadly to its citizens as Estonia has done, or it can choose to close its cyber borders to outside influences as North Korea has done.

In conjunction with this right, States are obligated to recognize this right and not interfere with the domestic cyber decisions of another State. For example, except as provided by international law, one State cannot place limits on the ability of another with respect to its cyber development and capabilities. States can, either bilaterally or multilaterally, agree to collaborate on cyber activities or place limits or constraints on such development between or among themselves.

Because of the place of a State on the international sphere, States may express their intent and work toward the development of State practice, either alone or in conjunction with others. In line with this, many States have actively participated in international fora, such as the U.N.-sponsored Group of Government Experts, and regional fora, such as the Shanghai Cooperation Organization or the Council of Europe. As with any international agreement, States have the obligation to negotiate in good faith and to comply with their international obligations, once undertaken.

One of the recently developing pressures on the idea of cyber sovereignty is the movement to recognize a human right to the Internet. If the time comes that such a human right is recognized and accepted by States, that right will, of course, impose obligations on the sovereign decisions of each State, constraining State action that might affect the enjoyment of that human right by its population.

Additionally, a State's exercise of sovereignty over cyber resources can be directed or limited by the U.N. Security Council through the power granted to it in the U.N. Charter. States have a duty to comply with Security Council resolutions, even if they limit the exercise of sovereignty over cyber issues. Additionally, States must comply with human rights obligations, even if it limits their exercise of sovereignty.

For example, assume State A contracts for the use of cyber capabilities from State C. Assume further that State A is using cyber means to incite human rights abuses in State B through the cyber infrastructure provided by State C. If the Security Council orders State C to stop allowing State A to use its cyber infrastructure, State C must comply.

2. Equality

Just as States are equals under the doctrine of sovereignty, each State exercises its sovereign cyber prerogatives on an equal plane with all others. Each State, regardless of its cyber capabilities, has the same right to exercise sovereignty over its territory as any other State. However, in doing so, conflicts often arise between States. Certain obligations attach to States in these disputes.

First, States have an obligation to resolve peacefully cyber disputes that may endanger international peace and security. If States attempt to resolve cyber disputes that don't endanger international peace and security, they must do so peacefully.
For example, if State A is using cyber means to harm State B, and that action is endangering international peace and security, both States have an obligation to resolve the dispute peacefully. Alternatively, if State A is using cyber means to steal information from State B, but that theft of information does not endanger international peace and security, a dispute may arise, but there is no obligation to try to settle that dispute. However, if attempts to settle that dispute are made, those methods must be peaceful.

Second, in its cyber activities, a State must exercise due regard for the rights of other States. For example, assume a State wants to increase its cyber security. In an effort to do so, it decides to aggressively monitor cyber threats across the World Wide Web. That State has the right to do so, so long as its activities do not violate the rights of other sovereign States.

D. The Way Ahead

This principle of sovereign equality raises some lingering issues that continue to be the focus of the international community. Because States are sovereign and equal, each State is able to develop its cyber capabilities based on its own best interest. Further, each State has no obligation to get involved in other States’ domestic cyber issues unless it chooses to do so. However, there is a great deal of discussion about cyber collaboration, particularly as it relates to less developed countries.

The U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security recently stated in its report that “confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective.” This collaboration would “be designed to share best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability.”

Information sharing and capacity building claims revolve mostly around calls for “ensuring global [information and communications technology] security,” and many States have responded favorably to some of these ideas. In the Department of Defense's Cyberspace Policy Report, the Department of Defense stated,

In collaboration with other U.S. Government agencies, Allies and partners, [the Department of Defense] pursues bilateral and multilateral engagements to develop further norms that increase openness, interoperability, security, and reliability. International cyberspace norms will increase stability and predictability of state conduct in cyberspace, and these norms will enable international action to take any required corrective measures.

The balance that will have to be struck between the exercise of sovereign prerogative with respect to cyber activities and the benefits of information and security sharing for the health of the Internet will continue to be a vexing issue for the foreseeable future. For now, there is no obligation to engage in information and security sharing, but much pressure to do so.

Finally, the equality of States means that each State has an equal vote in the discussion of how to resolve lingering cyber issues. For example, a group of States headed by Russia recently proposed a “code of conduct” for cyber activities. Other nations, such as the United States, did not support such an initiative. States may choose to band together in regional alliances with respect to cyber activities or may take unilateral action. No consensus is required in a system of sovereign equality.
II. STATES EXERCISE SOVEREIGNTY OVER TERRITORY, PERSONS, AND ACTIVITIES

Though sovereignty manifests itself in many different ways, it almost always means that a sovereign has some kind of territory over which it exercises ultimate control. As clearly stated in one of the seminal treatises on international law, “The corollaries of the sovereignty and equality of states [include] a jurisdiction, prima facie exclusive, over a territory and the permanent population living there . . . ”

*292 The rest of Part II will discuss the sovereign rights and obligations with respect to territory and persons, and then apply these rights and obligations to cyberspace, including identifying particular issues that remain unsettled.

A. Territory

Sovereignty over a territory denotes certain rights and corresponding obligations associated with that specific territory.

1. Rights

Perhaps the most important sovereign right over territory is the exclusivity of authority. As von Heinegg has stated, “territorial sovereignty protects a State against any form of interference by other States.” Sovereigns alone exercise this right and are only encroached upon through consensual divestiture of authority. Even the UN Charter grants States protection under Article 2(7) against intervention from the United Nations, and other States in certain matters, concerning issues that fall within a State's domestic jurisdiction.

Sovereignty over territory necessarily implies sovereignty over things found on or within territory. For example, “[O]bjects owned by a State or used by that State for exclusively non-commercial government purposes are an integral part of the State’s sovereignty and are subject to the exclusive jurisdiction of that State if located outside the territory of another State.” This exclusivity of jurisdiction would also apply to objects that have sovereign immunity, wherever located. Additionally, objects not owned by the State but located within the State's territory are subject to the State's regulation. This would include both real and personal property.

States also exercise authority to control their geographic borders. This implies that “the State is entitled to control access to and egress from its territory,” which “seems to also apply to all forms of communication.”

*293 2. Obligations

The principle of sovereign equality entails an obligation of all States to respect the territorial sovereignty of other States. As the ICJ noted in the Nicaragua judgment, “[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations.”

Another extremely important obligation that each sovereign State has is to not knowingly allow its territory to be used to harm another State. This obligation is well founded in international law and stated clearly in the ICJ's Corfu Channel case where the court says a State may not “allow knowingly its territory to be used for acts contrary to the rights of other States.”
Accordingly, States are required under international law to take appropriate steps to protect the rights of other States. This obligation applies not only to criminal acts harmful to other States, but also, for example, to activities that inflict serious damage or have the potential to inflict such damage on persons and objects protected by the territorial sovereignty of the target State.

These obligations, as applied to cyber operations, generate interesting discussion, as will be covered in further detail below. While it is mostly clear how they apply in the non-cyber world, cyber operations have caused many to rethink the practical application of these foundational sovereign obligations.

**B. Persons**

The ability of a sovereign State to assert power over persons has been uncontroversial since the genesis of statehood. However, the bounds of that assertion have often been contested, including in a seminal case decided by the Permanent Court of International Justice (PCIJ), the precursor to the ICJ. In *S.S. “Lotus”*, a dispute arose between France and Turkey over Turkey’s assertion of authority in the case of an accidental collision at sea. The Court in that case determined that the public international law regime was fundamentally permissive and that where there was no positive restriction, sovereigns were generally free to assert their authority over individuals in the absence of a specific proscription from doing so.

While that specific decision of the PCIJ has been limited under modern international law, a State’s current ability to exercise sovereignty applies to all legal persons within its territory and some outside its territory, such as its citizens who are abroad. This means that a State’s sovereign rights and obligations extend to both State and non-State actors who meet those qualifications.

1. Rights

Sovereign States’ ability to exercise prescriptive jurisdiction (territorial, nationality, protective, passive personality, and universal) over both State and non-State actors is guided by international law. These accepted limitations represent the modern constraints on the assertion of such jurisdiction. Conflicting assertions are normally resolved through the principles of comity. As the U.S. Supreme Court recently described it, “[A]merican courts have long held that application of [American] antitrust laws to foreign anticompetitive conduct is nonetheless reasonable, and hence consistent with principles of prescriptive comity, insofar as they reflect a legislative effort to redress domestic antitrust injury that foreign anticompetitive conduct has caused.”

States have also established international agreements that have created methodologies for the exercise of jurisdiction over persons. These agreements include both multilateral agreements such as the European Cybercrime Convention and bilateral agreements such as extradition treaties. They provide a mechanism for sovereign States to assert rights over individuals in situations of conflicting claims.

2. Obligations

The ability to exercise rights of legal persons also brings obligations to do so. Recall the maxim that States must prevent their territory from knowingly being used to harm the territory of another. That harm is almost always generated by some actor, taking some action. If States have the obligation to prevent known trans-boundary harm, they have to accept
the corresponding obligation to exercise control and authority over those within their power who are causing that trans-boundary harm. This obligation applies to both State and non-State actors.

The ICJ provided insight into the application of this obligation to non-State actors in *Armed Activities on the Territory of the Congo.* The Court was unwilling to assign responsibility to Zaire for not preventing the activities of certain armed groups because the government was not capable of doing so. However, the clear implication of the Court's decision is that if the government had been capable, it would have had the obligation to do so.

*296 C. Application to Cyberspace*

One of the potential difficulties with applying sovereignty to cyberspace is the claim that cyberspace is a virtual world and does not lie within any national sovereignty. In other words, skeptics claim that the activities that take place in cyberspace do not always fall under a State's jurisdiction. The next two Subparts will analyze these arguments with respect to territory and persons.

1. Territory

Some have likened cyberspace to the commons, such as the high seas, and proposed that a similar legal regime should apply. The argument is that because cyberspace does not fall within any State's territory, it is not subject to any State's sovereignty. The authors of the *Tallinn Manual* responded to this issue by arguing that “although no State may claim sovereignty over cyberspace per se, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure.”

Cyber infrastructure is composed of servers, computers, cable, and other physical components. These components are not located in cyberspace, but on some State's territory. It seems clear that a State has jurisdiction and exercises sovereign authority over these components that are located within its territorial boundaries. A State also exercises jurisdiction over cyber infrastructure outside its geographic boundaries if it exercises exclusive control over that cyber infrastructure, such as with cyber infrastructure on a State warship on the high seas. The scope of territorial sovereignty in cyberspace includes the cyber infrastructure “located on a State's land area, in its internal waters, territorial sea and, where applicable, archipelagic waters, and in national airspace” but does not extend to its exclusive economic zone or on the continental shelf where States only exercise “sovereign rights.”

The law is at least settled enough with respect to cyber activities that the authors of the *Tallinn Manual* listed as its first “black letter” rule, “A State may exercise control over cyber infrastructure and activities within its sovereign territory.” One of the *Tallinn* authors has also written that “State practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty nor from the exercise of State jurisdiction.” Nor does connecting that infrastructure to the World Wide Web connote some kind of waiver of sovereignty. In fact, the practice of States is just the opposite -- the practice of States has made it clear that they will continue to exercise territorial sovereignty over their cyber infrastructure.

This authority comes with corresponding duties and obligations. One of the primary obligations is that a State has an obligation not to knowingly allow its cyber infrastructure within its territory or under its exclusive control to cause trans-boundary harm. This obligation has been accepted to apply to radio telecommunications and was recently recognized as a rule by the authors of the *Tallinn Manual.*
This obligation has also been stated in multiple official State comments. For example, according to China, sovereign States “have the responsibilities and rights to take necessary management measures to keep their domestic sovereign and related infrastructure free from threats, disturbance, attack and sabotage.” 162 Similarly, India has stated, By creating a networked society and being a part of [a] global networked economy, it is necessary for nation states to realize that they not only have a requirement to protect their own ICT infrastructure but at the same time have a responsibility to ensure that their ICT is not abused, either covertly or overtly, by others to target or attack the ICT infrastructure of another nation state. 163

Likewise, Russia has stated that “States and other subjects of international law should refrain of [sic] such actions against each other and should bear responsibility at international level for such actions in information space, carried out directly, under their jurisdiction or in the framework of international organizations of their membership.” 164 Finally, the U.S. government’s 2011 International Strategy for Cyberspace calls on States to “recognize the international implications of their technical decisions, and act with respect for one another’s networks and the broader Internet.” 165

*298 These and similar statements, combined with limited State practice, have led many commentators 166 to argue, States have an affirmative duty to prevent cyberattacks from their territory against other states. This duty actually encompasses several smaller duties, to include passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states of cyberattacks that originated from within their borders. 167

The kinds of acts that equate to trans-boundary harm might include attacks on networks, exploitation of networks, and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy. 168 At this point, it is still unclear under the law as to whether the mere transit of data through a particular nation’s infrastructure rises to the level of a prohibited activity, even if the data eventually results in harm to another State. 169

Note that the obligation only triggers if the State from whose territory the harm originates has knowledge of the harm. 170 When States have knowledge of the harmful acts, they have a duty to stop them. 171 Knowledge might be imputed to the State if State agents or organs, such as intelligence or law enforcement agencies, know of the harm emanating from the State’s cyber infrastructure, even if those agents or organs choose to not inform other agencies in the government. 172

There may also be times when neither a State nor its organs or agents have actual knowledge but should have had knowledge, given the circumstances. In the ICI’s Corfu Channel case, the court held Albania liable for harm to England, even though there was no direct evidence that Albania knew of the harm. In that case, the court concluded that given the circumstances, Albania must have known about the emplacement of the mines that caused the harm. 173 The “must have known” standard is higher than a “should have known” standard but demonstrates that proving actual knowledge is not required. As for States who “should have known,” international law is still unclear as to the obligation of such a State. 174 However, von Heineg is willing to allow a rebuttable presumption of actual or constructive knowledge if “a cyber attack has been launched from cyber infrastructure that is *299 under exclusive government control and that is used only for non-commercial government purposes.” 175

There is currently an ongoing discussion as to whether a State’s responsibility to prevent knowing cyber harm creates a duty to monitor networks in order to “know” when cyber harms exist. 176 In other words, if such a responsibility exists, if State A knows that its infrastructure is being used to cause trans-boundary harm to State B, State A has an obligation to stop the harm. 177 In order to effectively comply with that obligation, there is an emerging norm that State A has an
obligation to monitor its cyber infrastructure and take proactive measures to prevent harm from emanating from cyber infrastructure over which State A exercises sovereignty. However, this emerging norm is still quite controversial, particularly when considered in light of potential human rights obligations that might be compromised in the process of monitoring.

Until that norm becomes generally accepted, target States will have to find ways to determine the level of knowledge of States from whose territory harmful cyber effects originate before allocating responsibility. In the current view of the United States,

[Department of Defense (DoD)] adheres to well-established processes for determining whether a third country is aware of malicious cyber activity originating from within its borders. In doing so, DoD works closely with its interagency and international partners to determine: [(1)] The nature of the malicious cyber activity; [(2)] The role, if any, of the third country; [(3)] The ability and willingness of the third country to respond effectively to the malicious cyber activity; and [(4)] The appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstances.

In addition to the obligation to prevent trans-boundary harm, a State has an obligation to cooperate with the victim State in the event of adverse or unlawful cyber effects from cyber infrastructure located in its territory or under its exclusive governmental control when it may affect international peace and security. A State may also have a treaty obligation to establish criminal information sharing and criminal processing arrangements as a matter of domestic law.

This obligation to cooperate is based on the U.N. Charter and ICJ opinions, and is also confirmed in the U.N. General Assembly's Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations. The obligation to cooperate with respect to cyber incidents is also enshrined in the European Convention on Cybercrime, which has forty-two States parties and an additional eleven signatory States.

This norm of cooperation only requires States to cooperate when the adverse or unlawful cyber incident originates from infrastructure within the territory or under its exclusive governmental control or when the unlawful cyber incident transits the cyber infrastructure in the State's territory or under its exclusive government control. Both conditions must be met for the duty to be applicable. No specific standard for the level of cooperation is clearly agreed upon, but the general consensus is that States must exercise good faith when fulfilling this duty.

As an example, if a cyber incident originates in State A and threatens State B's critical infrastructure such that there is a threat to international peace and security, both State A and State B have a legal duty to cooperate to peacefully resolve that incident.

As with the obligation concerning trans-boundary harm, the obligation to cooperate also has a number of unresolved issues. Most relevant to this Article is the fact that historical State practice does not demonstrate that States accept the obligation to cooperate in any meaningful way. Again, the 2007 situation between Estonia and Russia is instructive. Estonia found Russia's response to its queries and requests for assistance unhelpful and protective of Russian interests.

2. Persons
The U.S. Department of Justice's recent indictment of five members of the Chinese Army for cyber hacking represents a significant shift from the methodology States have traditionally used in dealing with State-sponsored cyber activities. For the United States to move away from its normal diplomatic approach and invoke domestic criminal law as a means of deterring State-sponsored cyber activities is a definite policy shift. Certainly, it is improbable that the indictment will result in any convictions as China and the United States do not have an extradition treaty and China has signaled no intention to honor such a request anyway. However, the idea that States will use domestic criminal law as a tool to deter other States who are engaged in harmful cyber activities is a potentially interesting development. The use of criminal law for non-State actors, on the other hand, is the norm, however ineffective.

It seems clear that in addition to State actors, "terrorist groups and even individuals, [sic] now have the capability to launch cyber-attacks, not only against military networks, but also against critical infrastructures that depend on computer networks." And the results of such actions can be catastrophic. "[M]alicious actors, state and non-state, have the ability to compromise and control millions of computers that belong to governments, private enterprises and ordinary citizens." The threat is such that [the President's May 2011 International Strategy for Cyberspace states that the United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these national security and vital national assets as necessary and appropriate."

The fact that cyber operations may be initiated by a vast array of persons implicates the States from which those persons take those actions. Every time there is a victim-State, there is a State from which the action was initiated and often a State or States through which the activity passed. In each case, those States have not only the right to control their citizens and others who might be involved, but also the obligation to do so. When persons take actions from within a State that harm another State, the State from which the harm originated has an obligation to try to stop those actions, once the State has knowledge. If a State is monitoring its networks and knows in advance, it can act preemptively to stop that activity before it emanates from within its sovereign territory. Additionally, as stated above with respect to controlling actions, a State can take proactive measures to discourage non-State actors by "passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-States of cyberattacks that originated from within their borders."

**D. The Way Ahead**

Applying a State's sovereign rights and obligations to persons with respect to cyber activities emphasizes the key role States must play in the way ahead for cyberspace. As the community of States moves forward, States will have to determine how the exercise of those sovereign rights and obligations can best be managed to accomplish each State's purposes.

For example, there are a number of issues revolving around the obligation to prevent trans-boundary harm. One of these issues stems from the fact that international law allows for some de minimis imposition on the rights of other States. It is unclear generally what the limit of acceptable de minimis harm is, but this is particularly unclear in cyberspace, where it is accepted that most cyber activities will not rise to the level of a use of force. As time progresses, State practice will indicate what the acceptable amount of de minimis harm is and where that line is generally crossed. Currently, that line is quite high because States are unwilling to respond in forceful ways to cyber activities. The shift in U.S. policy to apply domestic criminal remedies reflects that at least some States are not comfortable with the current paradigm. States' unwillingness to accept State-sponsored cyber activities, even those that are far below the use of force,
seems to be waning. The future will undoubtedly bring more proactive measures to deter States from conducting cyber activities and reduce the acceptable level of de minimis cyber harm.

Another current issue that will likely come to the fore in the near future concerns the knowledge requirement for the trans-boundary harm obligation. While the law is clear that some form of knowledge, whether actual or constructive, is required for responsibility, the law is unclear as to the responsibility of a State that chooses not to invest in cyber capabilities on purpose, in an effort to remain blind to its obligations.204 This issue of the level of knowledge, and responsibility to seek knowledge, will need to be resolved by State practice over time. As the duty to monitor and prevent continues to emerge, States will have to accept greater responsibility under a constructive knowledge standard and a State's ability to practice willful blindness will disappear. The pressures of the increasing availability of technology and the rising awareness of cyber activities will aid in this movement.

Finally, though there is a clearly recognized rule of international law on the acceptance of responsibility for trans-boundary harm, State practice in the cyber area has been inconsistent at best, and directly non-compliant in many cases.205 Particularly in the area of cyber operations that are generated from within a State's borders, there is a mixed history on responsible States' willingness to accept responsibility.206 Though this trend could actually go either way, it seems likely that the harms that are possible through cyber activities will eventually outweigh the benefits that States accrue by having freedom of action. Thus, particularly in light of the fact that non-State actors and even lone individuals can harness State-level violence through the use of cyber tools, States will soon find it in their best interest *304 to regulate themselves in order to protect themselves not only from other States, but from non-State actors as well.

CONCLUSION

An analysis of the international doctrine of State sovereignty demonstrates that many of those norms are directly applicable to cyber operations and can easily be applied with respect to States. In fact, the recently published Tallinn Manual concludes that principles of sovereignty can be applied and does so apply them.207

However, there are still areas where State practice has presented difficulties, such as the area of accepting responsibility for trans-boundary harm, the emerging principles of a duty to monitor and prevent, and the duty to apply due regard to a State's cyber activities.

It seems clear, though, that the future will provide greater clarity as incidents of state cyber activities become more widespread and the information more available to the public. At that point, the way ahead is likely to demonstrate that the doctrine of sovereignty continues to apply to cyber operations.

Footnotes

a1 Associate Professor, Brigham Young University Law School. The author would like to thank the staff of the Texas International Law Journal for hosting an excellent symposium and the attendees for their insights and comments to the author's presentation. Additionally, Grant Hodgson and Brooke Robinson provided excellent research and review assistance for this Article.

1 Gary D. Brown, The Wrong Questions About Cyberspace, 217 MIL. L. REV. 214, 225-26 (2013). Gary Brown was the first Staff Judge Advocate (legal advisor) for the newly formed United States Cyber Command. Id. at 214.

Cyber Sovereignty: The Way Ahead, 50 Tex. Int'l L.J. 275


7 The continuing application of international law to cyber capabilities has led one scholar to conclude:

This does not necessarily mean that the rules and principles of international law are applicable to cyberspace in their traditional interpretation. Because of the novel character of cyberspace, and in view of the vulnerability of cyber infrastructure, there is a noticeable uncertainty among governments and legal scholars as to whether the traditional rules and principles are sufficient to provide answers to some worrisome questions.

Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, 89 INT'L L. STUD. 123, 127 (2013). China, Russia, Tajikistan, and Uzbekistan seem to believe that new treaties governing cyber conflict are needed. See Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations, Letter dated 12 Sept. 2011 to the Secretary-General, U.N. Doc. A/66/359 (Sept. 14, 2011) ("China, Russia, Tajikistan and Uzbekistan have jointly elaborated in the form of a potential General Assembly resolution on an international code of conduct for information security and call for international deliberations within the United Nations framework on such an international code, with the aim of achieving the earliest possible consensus on international norms and rules guiding the behaviour of States in the information space."


8 See generally Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2010), transmitted by Note of the Secretary-General, U.N. Doc. A/65/201 (July 30, 2010) [hereinafter Int'l Sec. Grp.] (chronicling States' approaches to cybersecurity); U.N. Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) [hereinafter Developments in the Field of Information and Telecommunications] (reporting on how States have responded to the security concerns surrounding new developments in the fields of information and telecommunications).

9 See, e.g., generally Forrest Hare, Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?, in THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE 88 (Christian Czesseck & Kenneth Geers eds., 2009); Andrew Lioropoulos, Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?, in PROCEEDINGS OF THE 8TH INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY 136 (Douglas Hart ed., 2013); von Heinegg, supra note 7; Sean Kanuck, Sovereign Discourse on Cyber Conflict.


Brown, supra note 1, at 218.

TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 1 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]. The Author was a member of the international group of experts that drafted the Manual.


See supra notes 2-5 and accompanying text.

See Ruus, supra note 2 (discussing lack of Russian cooperation following the attack).


See David Hricik, Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail, 11 GEO. J. LEGAL ETHICS 459, 466-70 (1998) (outlining the complex process through which information is fragmented and disseminated through the internet according to the best path available, creating a random set of transmission paths at any moment).


See id. (discussing how the difficulty of attributing cyber attacks enables cyber attackers).

See id. at 781 (emphasizing the ability of non-State actors to carry out attacks and “harness the power of cyber weapons and use them at their discretion” without the threat of retribution).

See Hricik, supra note 16, at 467 (noting that the internet “is based on TCP/IP (Transfer Control Protocol/Internet Protocol) routing of information packets through unpredictable paths through interconnected networks linking millions of computers.” (internal quotation marks omitted)).

See id. at 469 (explaining how an email can “be broken into hundreds or thousands of packets, each potentially traversing several different networks around the globe” before reaching its destination (internal quotation marks omitted)).

Id.


WITT, *supra* note 29, at 2 (“President Lincoln will issue Lieber’s code as an order for the armies of the Union. He will deliver it to the armies of the Confederacy, too, and expect them to follow the rules he has set out. The code will be published in newspapers across the country and distributed to thousands of officers in the Union Army.”).


See BOBBITT, *supra* note 26, at 508 (noting that in the aftermath of the Thirty Years War, “[t]he extension of the maxim *cuius regio eius religio* imposed common restrictions on states, adumbrating the emergence of a new society of states characterized by their sovereign equality”).


E.g., John Alan Cohan, Sovereignty in a Postsovereign World, 18 FLA. INTL L. 907, 908-09 (2006); Reisman, supra note 26, at 866.

CRAWFORD, supra note 39, at 448.


Id.

Samantha Besson, Sovereignty, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW para. 119 (2011). Sovereignty is generally characterized as the “powers and privileges resting on customary law which are independent of the particular consent of another state.” CRAWFORD, supra note 39, at 448.


Besson, supra note 45, para. 75.


For example, during times of international armed conflicts, States have to treat prisoners of war in accordance with the Geneva Conventions, rather than any potentially applicable domestic law. See generally Geneva Convention on Prisoners of War, supra note 33.


IAN BROWN LI, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 289 (7th ed. 2008) (“The sovereignty and equality of states represent the basic constitutional doctrine of the law of nations....”); Michael J. Kelly, Pulling at the Threads of Westphalia: “Involuntary Sovereignty Waiver” -- Revolutionary International Legal Theory or Return to Rule by the Great Powers?, 10 UCLA J. INTL L. & FOREIGN AFF. 361, 364 (2005) (“Under classic Westphalian theory, the base maxim upon which foreign relations are built is the proposition that all states are equal and must reciprocally respect each other's sovereignty.”).
CRAWFORD, supra note 39, at 447 ("The corollaries of the sovereignty and equality of states [include]... a duty of non-intervention in the area of exclusive jurisdiction of other states....").

Ila?cu v. Moldova, 2004-VII Eur. Ct. H.R. 1, para. 312 ("[J]urisdiction is presumed to be exercised normally throughout the State's territory.").

For example, lawful countermeasures or actions taken in self-defense would allow a nation to interfere with another State's sovereignty. See U.N. Charter art. 51 (allowing a right of individual or collective self-defense in the event of an armed attack against a Member State of the United Nations).

E.g., Corfu Channel, 1949 I.C.J. at 35 ("Between independent States, respect for territorial sovereignty is an essential foundation of international relations.").

See infra Part I.B.2.

U.N. Charter art. 2, para. 1.

CRAWFORD, supra note 39, at 448 & n.9.

U.N. Charter art. 2, para. 1.

CRAWFORD, supra note 39, at 447.

See, e.g., Philippines Seeks Quick UN Ruling on South China Sea Dispute, S. CHINA MORNING POST, June 19, 2014, http://www.scmp.com/news/asia/article/1536058/philippines-seeks-quick-un-ruling-south-china-sea-dispute ("China claims most of the South China Sea, including waters near the shores of its neighbours, which has led to escalating territorial disputes."); Russell Hotten & Alix Kroeger, Ukraine-Russia Gas Row: Red Bills and Red Rags, BBC (June 16, 2014), http://www.bbc.com/news/world-europe-26987082 (stating that the gas conflict is a "power struggle between the interim Ukrainian government, which leans towards the EU, and Russia, which wants to keep Ukraine firmly within its sphere of influence").

CRAWFORD, supra note 39, at 449 (citing GEORGE ORWELL, ANIMAL FARM 90 (1945)).

Liaropoulos, supra note 9, at 137–38 (citation omitted).

See Todd B. Adams, Is There a Legal Future for Sustainable Development in Global Warming? Justice, Economics, and Protecting the Environment, 16 GEO. INT'L ENVTL. L. REV. 77, 97 (2003) ("[The world] is to be shared by all generations in accordance with the limited rights and necessary obligations of a user of the natural resources or the trustee of the natural resources.... [P]lanetary rights are group rights to equal access to the commons." citing EDITH BROWN WEISS, IN FAIRNESS TO FUTURE GENERATIONS: INTERNATIONAL LAW, COMMON PATRIMONY, AND INTERGENERATIONAL EQUITY 96 (1989)).

See Inaamul Haque & Ruxandra Burdescu, Monterey Consensus on Financing for Development: Response Sought from International Economic Law, 27 B.C. INT'L & COMP. L. REV. 219, 249–50 (2004) ("Under customary international law, principles of sovereignty support a state's clear right to regulate commercial activities within its borders. This power is extensive and encompasses such issues as capacity to engage in business, forms of business enterprises, conditions of continuance of a business, and regulations of capital markets as well as those of foreign capital inflows and outflows.").

E.g., George K. Walker, Defining Terms in the 1982 Law of the Sea Convention IV: The Last Round of Definitions Proposed by the International Law Association (American Branch) Law of the Sea Committee, 36 CAL. W. INT'L L.J. 133, 168–69 (2005) ("Article 87(2) declares that the high seas freedoms listed in Article 87(1)... 'shall be exercised by all States with due regard of the interests of other States in their exercise of the freedom of the high seas, and also with due regard for the rights under [the] Convention with respect to activities in the Area.'" (alteration in original) (quoting U.N. Convention on the Law of the Sea, supra note 54, art. 87(2))).


Walker, supra note 72, at 174.

U.N. Charter art. 2, paras. 3-4; Id. arts. 33-38.


Aerial Incident of 10 August 1999 (Pak. v. India), Judgment, 2000 I.C.J. 12, para. 53 (June 21).

See id. para. 22 (noting claims to resolve disputes peacefully in cited bilateral and multilateral treaties).

U.N. Charter art. 33, para. 1.

G.A. Res. 2625 (XXV), supra note 80.


See TALLINN MANUAL r. 1 (observing that sovereignty gives States the exclusive right to control cyber infrastructure and cyber activities within their boundaries).

See id. (delineating exclusive rights associated with State sovereignty in cyberspace).


90  Int'l Sec. Grp., supra note 8, at 7-8.
93  See, e.g., Aerial Incident of 10 August 1999 (Pak. v. India), Judgment, 2000 I.C.J. 12, para. 53 (June 21) (“The Court's lack of jurisdiction does not relieve States of their obligation to settle their disputes by peaceful means.... They are [ ] under an obligation to seek [a peaceful settlement], and to do so in good faith....”); G.A. Res. 2625 (XXV), supra note 80, at 123 (reaffirming U.N. Charter principles related to peaceful resolution of conflicts); Draft Declaration on Rights and Duties of States, G.A. Res. 375 (IV), annex art. 13, U.N. GAOR, 4th Sess., U.N. Doc. A/1251, at 67 (Dec. 6, 1949) (“Every State has the duty to carry out in good faith its obligations arising from treaties and other sources of international law....”); Markus Kotzur, Good Faith (Bona Fide), in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, supra note 45, paras. 11-14 (discussing treaties that require good-faith negotiation).
95  U.N. Charter art. 25 (“The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter.”).
96  See, e.g., International Covenant on Civil and Political Rights, opened for signature Dec. 16, 1966, 999 U.N.T.S. 171 (establishing the civil and political rights of all individuals as well as States' obligations to protect those rights).
97  See, e.g., Lesley Wroughton & Michael Martina, Cyber Spying, Maritime Disputes Loom Large in U.S.-China Talks, REUTERS (July 8, 2014), http://www.reuters.com/article/2014/07/08/china-usa-idUSL4N0P0MT20140708 (noting increased tensions between the United States and China regarding the territorial scope of cyber activities).
98  See U.N. Charter art. 2, para. 3 (“All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.”).
99  Id.
100  See supra notes 72-78 and accompanying text (discussing the duty of due regard and its broad applicability under international law).
101  Int'l Sec. Grp., supra note 8, para. 15.
102  Id. para. 14.
103  E.g., id. para. 17.
on information and communications technology security in order to reduce the possibility of a cyber incident destabilizing their bilateral relationship).


Wu & Zhao, supra note 7.

Healey, Breakthrough or Just Broken?, supra note 7.

See JOHN LYONS, ESTABLISHING THE INTERNATIONAL CYBER SECURITY PROTECTION ALLIANCE IN ASIA PACIFIC (ICSPA APAC) 1 (2014) (announcing the establishment of an alliance in the Asia Pacific to enhance online safety and security and provide governments and law enforcement agencies with resources and expertise to help them reduce harm from cyber crime).

Abraham D. Sofer et al., Cyber Security and International Agreements, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 179, 179 (The Nat'l Acad. Press ed., 2010) ("[C]urrent U.S. efforts to deter cyberattacks and exploitation -- though formally advocating international cooperation -- are based almost exclusively on unilateral measures.").

See Besson, supra note 45, para. 1 (defining sovereignty as "supreme authority within a territory.")

Id. para. 70 (referring to sovereignty as encompassing "ultimate authority and competence over all people and all things within [the sovereign's] territory").

CRAWFORD, supra note 39, at 447.

von Heinegg, supra note 7, at 124.

See Cohan, supra note 41, at 935 (explaining how States can willingly enter into agreements that undermine their domestic sovereignty by recognizing external authority structures).

U.N. Charter art. 2, para. 7; Besson, supra note 45, para. 88 ("The UN Charter also protects sovereign States' domaine réservé and prohibits other States' intervention on sovereign States' territory." (citations omitted)).

von Heinegg, supra note 7, at 130.

TALLINN MANUAL r. 4.

von Heinegg, supra note 7, at 124.

HENRY WHEATON, ELEMENTS OF INTERNATIONAL LAW § 77 (George Grafton Wilson ed., 1936) (1836).

Hare, supra note 9, at 92.

von Heinegg, supra note 7, at 124.


Corfu Channel (U.K. v Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

Id.

See, e.g., United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, paras. 67-68 (May 24) (describing the general obligation under international law for States to "ensure the most constant protection and security to each other's nationals in their respective territories." (internal quotation marks omitted)).
In the Trail Smelter case, the arbitral tribunal, citing the Federal Court of Switzerland, noted: “This right (sovereignty) excludes... not only the usurpation and exercise of sovereign rights... but also an actual encroachment which might prejudice the natural use of the territory and the free movement of its inhabitants.” Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1963 (1941) (first omission and part of second omission in original). According to the tribunal, “under the principles of international law... no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes... in or to the territory of another or the properties or persons therein, when the case is of serious consequence.” Id. at 1965.


See, e.g., Cohan, supra note 41, at 944 (“The concept of sovereignty... has previously been characterized as the right of a State to exercise supreme power over its territory and citizens, free from outside interference.”); von Heinegg, supra note 7, at 132 (“Moreover, according to the principles of active and passive nationality, a State is entitled to exercise its jurisdiction over the conduct of individuals that occurred outside its territory.”)


Id. at 18 (“International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.”).

See U.N. Convention on the Law of the Sea, supra note 54, art. 97 (“In the event of a collision or any other incident of navigation concerning a ship on the high seas, involving the penal or disciplinary responsibility of the master or of any other person in the service of the ship, no penal or disciplinary proceedings may be instituted against such person except before the judicial or administrative authorities either of the flag State or of the State of which such person is a national.”).

See Helen Stacy, Relational Sovereignty, 55 STAN. L. REV. 2029, 2050-51 (2003) (“Sovereignty attaches itself to the people of the state, not merely the state itself... Relational sovereignty places a higher obligation on the sovereign state to care for and regulate the behavior of its citizens both inside and outside state borders.”).

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402(1) (1986).

Id. § 402(2).

Id. § 402(3) & cmt. f.

Id. § 402 & cmt. g.

Id. § 404.

See INT’L BAR ASS’N, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION 11 (2009) (“The starting point for jurisdiction is that all states have competence over events occurring and persons (whether nationals, residents or otherwise) present in their territory... In addition, states have long recognised the right of a state to exercise jurisdiction over persons or events located outside its territory in certain circumstances, based on the effects doctrine, the nationality or personality principle, the protective principle or the universality principle.”).

See id. at 11-16 (discussing the different bases for a State’s exercise of extraterritorial jurisdiction).

Robert C. Reuland, Hartford Fire Insurance Co., Comity and the Extraterritorial Reach of United States Antitrust Laws, 29 TEX. INT’L L.J. 159, 161 (1994) (“In adopting a position that comity considerations may be relevant only in the case of a ‘true conflict,’ the Supreme Court effectively closes the door to the consideration of comity issues under any circumstances short of an actual conflict between U.S. and foreign law.”).

Convention on Cybercrime, supra note 92.


See, e.g., Cohan, supra note 41, at 939-40 ("Membership in the United Nations and in other international organizations means that the participating state accepts the right of its fellow members to intervene in its domestic affairs if it has failed in its most fundamental obligations to protect its own citizens..." (internal quotation marks omitted)); Worth, supra note 48, at 256 ("Article 12(2)(b) [of the Rome Statute] states that the Court will have personal (ratione personae) jurisdiction over the citizens of states that have become party to the [International Criminal Court].").


Id.

See David R. Johnson & David Post, Law and Borders — The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367, 1371 (1996) ("The power to control activity in Cyberspace has only the most tenuous connections to physical location.").

See, e.g., Id. at 1372 (arguing that "efforts to control the flow of electronic information across physical borders... are likely to prove futile").

See, e.g., Dan Hunter, Cyberspace as Place and the Tragedy of the Digital Anticommons, 91 CALIF. L. REV. 439, 517 (2003) ("[W]ith the intangible property of cyberspace, we can throw out our normal assumptions about private ownership of the resources and recognize that a commons system might be the most efficient use of the resource.").

See Johnson & Post, supra note 147, at 1370 ("The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules.").

TALLINN MANUAL r. 1 cmt. 1.

Id. gloss.

Id. r. 5.

von Heinegg, supra note 7, at 128 & n.17.

TALLINN MANUAL r. 1.

von Heinegg, supra note 7, at 126.

Id.

DEPARTMENT OF DEFENSE, STRATEGY FOR OPERATING IN CYBERSPACE, supra note 89, at 1.


Developments in the Field of Information and Telecommunications, supra note 8, at 3.

TALLINN MANUAL.

Kanuck, supra note 9, at 1591 (internal quotation marks omitted).

Id.

Id. at 1591 n.88.

OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE, supra note 37, at 10.


See OFFICE OF THE PRESIDENT, 1 NTERNATIONAL S TRATEGY FOR C YBERSPACE, *supra* note 37, at 12-14 (recognizing that cyberspace activities can have effects beyond borders and detailing initiatives that will be undertaken to protect the United States against threats posed by cyber criminals or States and their proxies).

von Heinegg, *supra* note 7, at 137.

*Id.* at 136.

*Id.* at 135-36.

*Id.* at 136.


See von Heinegg, *supra* note 7, at 151 (speculating hypothetically about whether constructive knowledge is sufficient to establish a violation).

*Id.* at 137. Note that von Heinegg clearly states that the presumption does not allow for attribution. *Id.*

See generally Jensen, *State Obligations*, *supra* note 127.

See *id.* at 13 (stating that in order to comply with the duty to control their cyber infrastructures, States have an emerging duty to monitor cyber activities within their territories in order to prevent or stop activities that are adversely or unlawfully affecting other States).

*Id.*

Cf. EKATERINA A. DROZDOVA, CIVIL LIBERTIES AND SECURITY IN CYBERSPACE 13 (2000), available at http://fsi.stanford.edu/sites/default/files/drozdova.pdf (“While a system for advanced monitoring, searching, tracking, and analyzing of communications may be very helpful against cyber crime and terrorism, it would also provide participating governments, especially authoritarian governments or agencies with little accountability, tools to violate civil liberties domestically and abroad.”).


In addition to those circumstances mentioned above where the maintenance of international peace and security is at risk, the duty to cooperate also applies to the solving of international problems of economic, social, cultural, or humanitarian character. U.N. Charter art. 1, para. 3. States also have a duty to cooperate in scientific investigation in Antarctica. The Antarctic Treaty, *supra* note 53, art. 2. The duty to cooperate also applies to the scientific investigation of outer space. Outer Space Treaty, *supra* note 55, art. 1. Finally, international cooperation applies to marine scientific research. U.N. Convention on the Law of the Sea, *supra* note 54, art. 143.

See, e.g., Convention on Cybercrime, *supra* note 92, art. 26, para. 1 (“A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for cooperation by that Party under this chapter.”).

U.N. Charter art. 1, paras. 1, 3; *Id.* art. 33, para. 1.
See, e.g., Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 102 (Apr. 20) (finding it vital for parties to comply with their procedural obligations under the 1975 Statute of the River Uruguay because cooperation is essential to the protection of the river).

G.A. Res. 2625 (XXV), supra note 80, at 123.

Article 23 requires that "[t]he Parties shall co-operate with each other" and provide mutual assistance, particularly with respect to investigations of cyber incidents. Convention on Cybercrime, supra note 92, art. 23.

See Kotzur, supra note 93, para. 16 ("One of the most basic principles governing the creation and performance of legal obligations, whatever their source, is the principle of good faith.").

See Schmitt, The Law of Cyber Warfare, supra note 12, at 273 ("A state's national interests undergird its consent or conduct.... States might seek, for example, to maximize power and influence at the expense of other states....").

See Ruus, supra note 2 ("[T]he Estonian State Prosecutor made a formal investigative assistance request, which Moscow rejected, alleging that procedural problems prevented cooperation.").


See Schmidt & Sanger, supra note 190 ("[President Obama and Defense Secretary Chuck Hagel] have attempted to engage the Chinese in a dialogue over norms for operating in cyberspace, a careful diplomatic dance that has gone on for several years. But Monday's action by the Justice Department marked an attempt to publically shame the Liberation Army....").


See Schmidt & Sanger, supra note 190 (describing how the Justice Department indicted five members of the Chinese People's Liberation Army and illustrating how this represents a U.S. policy shift on dealing with Chinese cyber activities).


Liaropoulos, supra note 9, at 136 (citation omitted).

Id. at 137.

DEPARTMENT OF DEFENSE, CYBERSPACE POLICY REPORT, supra note 105, at 2.

Jensen, Sovereignty and Neutrality, supra note 9, at 826-27.

Id.

Sklerov, supra note 166, at 62.
201 See Jutta Brunnée, Sic utere tuo ut alienum non laedas, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW para. 7 (2010) ("[T]he mere causation of transboundary harm does not transgress the sic utere tuo maxim.").

202 See TALLINN MANUAL r. 11 (defining the term “use of force” in the cyber context as an operation the scale and effects of which are comparable to non-cyber operations that would qualify as a use of force).

203 But see DEPARTMENT OF DEFENSE, CYBERSPACE POLICY REPORT, supra note 105, at 4 ("Finally, the President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include significant cyber attacks directed against the U.S. economy, government or military. As directed by the President, response options may include using cyber and/or kinetic capabilities provided by [the Department of Defense].").

204 TALLINN MANUAL r. 93.

205 See, e.g., discussion supra Part II.C.1 on Russia’s unwillingness to assist Estonia after the 2007 cyber attacks.

206 See, e.g., Sklerov, supra note 166, at 10 ("As may be expected, China and Russia reject these accusations.").

207 TALLINN MANUAL R. 1.
I. INTRODUCTION

When David Sanger and Ellen Nakashima officially broke the news that the United States and Israel had been involved in a long-term collaborative cyber operation focused on Iran and its nuclear development capabilities, they only confirmed what many had assumed for some time. In fact, with the discovery of Stuxnet in 2010, many scholars and practitioners had speculated on whether the use of the Stuxnet malware, if State sponsored, amounted to a “use of force” or even an “armed attack” under the UN Charter paradigm.

Some even began to consider the hypothetical legality of Stuxnet-type cyber actions within an armed conflict as opposed to a use of force or armed attack that would initiate an armed conflict. For these writers, the major issues revolved around the cyber tool’s compliance with the law of armed conflict (LOAC) and principles such as discrimination and proportionality. For example, Jeremy Richmond analyzed Stuxnet in light of these principles and concluded that whoever designed the malware did so with the clear intent to comply with the LOAC.

Even prior to the discovery of Stuxnet, a group of legal and technical experts were gathered by the Estonian Cooperative Cyber Defence Centre of Excellence to draft a manual, known as the Tallinn Manual on the International Law Applicable to Cyber Warfare. The Manual explores the international law governing the use of force—in both its jus ad bellum and jus in bello aspects—as applied to cyber operations conducted by States and non-State actors. Several key principles arose during the Manual discussions in relation to the principles of proportionality and precautions in and against attack, including a number of challenging aspects in applying these principles to cyber warfare. This article will discuss some of those interesting challenges.

Part II of the article will focus on the constant-care standard and how it applies to all cyber operations. Part III will look at the principle of proportionality with specific focus on the idea of indirect effects. Part IV analyzes the issue of feasibility with the precautionary standards. Part V analyzes State responsibilities under the obligation to take precautions against the effects of attacks. The article will conclude in Part VI.

A. Attack

Before embarkation on the above-mentioned analysis, some brief comments are necessary concerning the definition of “attack.” With the exception of Part II, which deals with the constant-care standard, the legal standards discussed below apply to an “attack.” Many LOAC principles apply only to situations of attack, such as the principle of proportionality. The idea of taking precautions in the attack assumes that there is an attack. The fundamental nature of “attack” underlies
many of the LOAC principles that govern cyber warfare, making it important to come to some understanding of the meaning of the word.

Paul Walker was one of the first to address this issue directly, in his article “Rethinking Computer Network ‘Attack.’” He notes that the word “attack” is defined in the 1977 Additional Protocol I (API) to the Geneva Conventions as “acts of violence” and states that this definition has become customarily binding even on non-parties to the Protocol. As a result, Walker argues that very few activities in cyber warfare will actually amount to an attack and will therefore not be governed by the principles of attack, such as proportionality.

The meaning of “attack” was also vigorously debated by Michael Schmitt, Chairman of the International Law Department of the U.S. Naval War College and leader of the Tallinn Manual project, and Knut Dörmann, representative of the International Committee of the Red Cross. In Schmitt’s view, an attack is something that results in death, damage, destruction or injury. Dörmann argued that anything that was aimed at civilians amounted to an “attack.” These views tend to mark the extremes of the debate. The Tallinn Manual softened Schmitt’s view somewhat by indicating that a cyber attack need not be characterized by the release of kinetic force.

Resolving the debate on the definition of attack may need to wait for more State practice. It is enough for this article to state that most of the law discussed here presupposes an “attack,” whatever that means. For example, in the absence of an attack, commanders are not required to apply the principle of proportionality.

**B. State and Non-State Actors**

In addition to the definition of “attack,” another important consideration is the involvement of non-State actors in cyber operations. One of the most intriguing aspects of cyber operations is that they allow non-State actors to relatively easily harness State-level violence. This undermines the Westphalian monopoly on the use of violence as few other weapon systems have done.

Other articles in this volume will address this question more directly, so little need be said here except to note that many of the standards discussed below only apply to States. To the extent that some organized armed groups might elect to be bound by LOAC principles, they would also be bound, but as a matter of law the majority of the discussion below applies to States.

**II. THE “CONSTANT-CARE” STANDARD**

Article 57 of Additional Protocol I is titled “Precautions in the Attack” and is generally believed to be binding on States in both international armed conflict and non-international armed conflict. However, the first subparagraph takes a much broader approach than just “attack.” It states that “In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.” The ICRC Commentary adds, “The term ‘military operations’ should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat.”

The term “military operations” is obviously meant to be much broader than the term “attack” and imposes a general legal requirement on militaries even when not attacking. The legal requirement is to exercise “constant-care,” but that term is not defined either in Article 57, the ICRC Commentary or generally in the LOAC. While the exact application of this principle in a specific military operation must be left to the commander, it seems clear that exercising constant care would at least mean that a commander cannot ignore effects on civilian population.
In the context of cyber operations, constant care would likely require a commander to maintain situational awareness at all times, including all *203 phases of the operation. When employing a cyber tool or conducting cyber operations, the commander would need to maintain oversight of the tool and be ready to adjust operations if the tool or operation began to have effects that the commander determined would have an illegal impact on civilians. This might be especially difficult in the cyber domain since virtually every cyber operation will traverse, affect, employ or damage civilian cyber infrastructure of some kind. 19

A contemporary application of this standard occurred in the case of the infamous Stuxnet malware. 20 Evidently, it was discretely targeted at Iranian nuclear facilities, but reports show that it spread much wider than that, presumably wider than the United States and Israel21 intended it to disseminate, which may have led to its discovery. Though no other damage was reported, the unintended spread of the virus at least implicates the constant-care standard and informs State practice on the issue.

Additionally, it appears that the Stuxnet malware was used in conjunction with another malware that has been termed “Flame.” Flame was “designed to secretly map Iran’s computer networks and monitor the computers of Iranian officials, sending back a steady stream of intelligence used to enable an ongoing cyberwarfare campaign.” 22 Flame was discovered by Iranian officials when Israeli government hackers were carrying out operations against Iranian oil ministry and export facilities. 23

Similar situations might lead a commander to argue that he cannot continue to monitor the network in order to exercise constant care for fear of being discovered. The LOAC allows no such exception in this case, though it does in others. 24 Therefore, it seems unlikely that a commander could *204 argue that he was relieved of his legal duty to maintain constant care for fear it might lead to discovery. Rather, commanders and all persons conducting cyber operations must recognize and accept the legal obligation to exercise constant care in all military operations, including cyber operations.

III. PROPORTIONALITY AND INDIRECT EFFECTS

The principle of proportionality is found in Article 51(5)(b) of API: 25

5. Among others, the following types of attacks are to be considered as indiscriminate:

... (b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

This principle is generally accepted as customary international law in international and non-international armed conflicts and is analyzed elsewhere in great length 26 so it needs no further discussion here.

Few would argue that the principle of proportionality does not apply to cyber warfare; instead the controversy centers on its application to specific cyber operations. 27 While all cyber operations are governed by the constant-care standard, the principle of proportionality will only apply to those cyber operations that amount to an “attack.” For those operations where the principle of proportionality does apply, two specific aspects of the rule deserve more detailed analysis: the understanding of “damage” and the problem of indirect effects.
*205 Preliminarily, it is important to keep in mind that civilians can never be made the object of attack and that the principle of proportionality limits commanders when, as the result of a lawful attack, civilians or civilian objects may be harmed. In order for such an attack to be lawful, the commander must determine that the death, injury and damage are not "excessive in relation to the concrete and direct military advantage anticipated." Though cyber attacks will inevitably have the ability to kill and injure civilians, the vast majority of known cyber operations have focused on or resulted in damage, hence the focus on the damage element of the legal standard.

Additionally, the requirement that the damage occur to civilian objects should be understood broadly. The vast majority of the Internet, including the cables, servers and routers, consists of civilian objects, which are owned, operated and maintained by civilians. Any damage to these elements of the Internet infrastructure would be considered civilian damage for purposes of the proportionality analysis.

Finally, although the drafters of 1977 Additional Protocol I certainly did not anticipate cyber warfare, they did recognize that electronic advances in technology would affect the way wars would be fought and their potential impacts on civilians. In the Commentary, the ICRC notes, "It was also pointed out that modern electronic means made it possible to locate military objectives, but that they did not provide information on the presence of civilian elements within or in the vicinity of such objectives." Though perhaps not entirely true in cyber warfare, this idea certainly impacts the application of proportionality to cyber attacks.

A. Damage to Civilian Objects

When considering kinetic weapons that result in heat, blast and fragmentation, the issue of defining damage is less controversial. However, when cyber tools are used to conduct an attack, determining what cyber actions amount to damage becomes more problematic. There are several approaches in determining what equates to damage in the cyber domain.

One approach would be to analogize from a kinetic attack and argue that if what occurs from a cyber operation would have been considered damage if accomplished by kinetic means, then the attack amounts to damage. *206 The advantage to this approach is that it places commanders in a comfortable position to apply known factors. Commanders have been applying the proportionality analysis to kinetic attacks their entire careers and will likely feel quite comfortable with this analysis.

However, there are many cyber actions that would not look at all like the results of a kinetic attack. For example, simply closing a computer's specific communication port normally used to communicate with another computer, while leaving the rest of the computer function untouched, is not a similar effect to what might be caused by a kinetic attack. Using the kinetic analogy approach, an extremely limited number of cyber attacks would cause damage.

Alternatively, one could take the view that any unauthorized intrusion into a computer or computer system results in a change to the computer or system and therefore equates to damage. In other words, the digital changes required to allow penetration into a computer would be damage under the principle of proportionality. This view would require a commander to essentially consider any effects on a computer system in his proportionality analysis.

This seems to go too far. The principle of proportionality was clearly not designed to exclude the possibility of any civilian casualties or damage, but only that which was excessive.

Finally, some have taken the view that damage also encompasses serious interruptions in functionality, such as would require replacing parts or reloading software systems. For example, in the kinetic analogy used above where a cyber attack shut down a communication port but left the rest of the computer unaffected, the computer would still turn on but

its actual functionality might be seriously affected. If functionality is considered when determining damage, the kinetic analogy would be of limited value.

*207 The functionality approach seems to be the best application of the proportionality rule to the cyber realm as it takes into account the unique aspects of cyber operations, without going so far as to make the proportionality analysis unwieldy for commanders to apply. Armed conflict has always included effects on civilians that have caused inconvenience, irritation, stress and fear, but these have traditionally not been part of the commander's analysis of damage required by the proportionality analysis. 32 By focusing on functionality, the commanders can easily understand the legal standard and apply it to modern cyber operations.

B. Indirect Effects

Gauging indirect effects in cyber warfare may prove to be one of the most difficult issues in applying proportionality. It is clear that a commander must consider the direct effects of his cyber attack. These direct effects are defined as the “immediate, first order consequences, unaltered by intervening events or mechanisms.” 33 In the cyber domain, this would include the effects on a computer that is shut down by a cyber attack or the damage to the centrifuges caused by the Stuxnet malware.

In contrast to direct effects, indirect effects are “the delayed and/or displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms.” 34 In the cyber domain, this would include damage that was not the intent of the attack, but that resulted from elements of the attack. In the case of Stuxnet, the malware infected many computers beyond its intended targets within Iran. Whatever damage might have resulted from these unintended infections might have been indirect effects. Another example might be a targeted attack on a military computer system that would shut the system down, but, because of the linkages between military and civilian systems, the malware is also likely to spread to the civilian systems and shut them down as well. Resulting indirect *208 effects are generally accepted as being included in the proportionality analysis. 35

Even in the cases mentioned above, for the damage to be considered in the proportionality analysis, it must have been expected. Indirect effects which were not expected to be excessive are not factored into the analysis. 36 In other words, this standard does not anticipate that a reviewer can come after the fact and assess the reasonableness of the commander's decision on the excessiveness of the indirect effects. Rather, any reviewer must assess the reasonableness of the commander's decision based on what the commander reasonably expected the effects to be, given the information he had at the time. 37

Considerations of expected effects have already affected known military operations. In the 2003 U.S. attacks on Iraq, cyber attackers for the United States considered attacking Saddam Hussein's financial accounts in an attempt to pressure him. The attacks were called off, however, when it was determined that the attacks would probably affect the European banking system and have negative repercussions. 38

Similar considerations would have to be made in the case that a prospective malware targeting military objectives was to be implemented via a portable storage device. The commander would have to determine whether or not the potential transfer of that same malware to civilian systems was expected, and then consider how much damage it was expected to cause. On the other hand, if that same malware was unexpectedly transferred into civilian systems, the commander would not be responsible for having misapplied the principle of proportionality.
A commander's ability to properly apply this rule is obviously tied back to the earlier discussion on constant care. Unless a commander is constantly *209 mapping and monitoring the targeted computer or network, he will not be able to make a reasonable assessment of what effects are expected.

IV. FEASIBILITY

The legal standard of feasibility appears in several places in the "Precautions in Attack" section of API 39 and applies to most types of attacks. 40 In various provisions, a commander must do "everything feasible" 41 or "take all feasible precautions." 42 During the ratification process, there was great debate about the term "feasible" and what it meant. 43 A number of representatives to the negotiating convention made specific comments about the meaning "feasible" was to have when applied as a legal standard. John Redvers Freeland, the head of the United Kingdom delegation, through several sessions stated that the words "to the maximum extent feasible" related to what was "workable or practicable, taking into account all the circumstances at a given moment, and especially those which had a bearing on the success of military operations." 44 Similarly, S.H. Bloemersen, a delegate from the Netherlands, stated that "feasible" should be "interpreted as referring to that which was practicable or practically possible, taking into account all circumstances at the time." 45 As a result, "feasible" is generally understood to mean that which is "practicable or practically possible, taking into account all circumstances ruling at the time." 46

*210 A. "Practicable or Practically Possible"

During the API negotiations mentioned above, the national representatives were anxious to set a standard that would require diligence on the part of the commander, but would not be one with which it was beyond his capability to comply. The resulting language of practicality was the eventual resolution, which seems to be a workable standard in applying precautions in the attack.

The application of "feasibility" to cyber attacks seems ultimately tied to technology. As a commander contemplates a potential cyber attack, his "feasible precautions" should require him to sufficiently map the networks to determine the effects of the attack, particularly on civilians and civilian objects. This is much like the duty of constant care, but should carry a heightened specificity when planning a specific attack.

If in the process of preparing a cyber attack, the commander is unable to determine the extent of the attack's effects, he cannot launch an attack that would otherwise be considered indiscriminate. Or, if an attacker is unable to gather sufficient information as to the nature of a proposed target system, he should limit the attack to only those parts of the system for which he does have sufficient information to verify their status as lawful targets. In other words, the feasibility limitation should not be used as a justification for conducting an attack.

B. Circumstances Ruling at the Time

Without detracting from the duty of constant care previously discussed, the commander's duty to do what is feasible is limited by his circumstances. This limitation on commanders' liability stems from the post-World War II prosecution of German general Lothar Rendulic. 47 General Rendulic conducted a scorched-earth policy in Finnmark to slow what he thought were swiftly advancing Russian troops. In the end, the Russians were not coming as quickly as Rendulic had thought and the destruction proved to be unnecessary. However, the Military Tribunal determined that the legal standard was "consideration to all factors and existing possibilities" as they "appeared to the defendant at the time." 48
*211 This same standard should apply to the understanding of “feasibility” in cyber attacks. While commanders are required to do everything practicable, the responsibility is limited to the circumstances as the commander knows them at the time. For example, if a commander has used his best technology to map a network and exercises continuous monitoring in preparation for the attack, he has not violated the law if, during the course of the attack, the malware spreads unexpectedly to a civilian network that the commander did not know was linked to the military system.

V. PRECAUTIONS AGAINST THE EFFECTS OF ATTACKS

In addition to considering precautions when conducting attacks, nations have an obligation to take precautions against the potential effects of attacks. 49 Unlike the provisions discussed above that govern the conduct of attacks, this standard is not only a wartime standard. Rather, it is a standard that applies to nations during peacetime, in anticipation that armed conflict might arise in the future that would affect civilians and civilian objects.

Article 58 reads:

The Parties to the conflict shall, to the maximum extent feasible:

(a) Without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;

(b) Avoid locating military objectives within or near densely populated areas;

(c) Take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations. 50

This provision of the law is binding on nations only in international armed conflict, and is considered part of customary international law. 51 The *212 cyber aspects of Article 58 have been thoroughly discussed recently. 52 It is sufficient here to say that it establishes two layers of responsibility. Initially, a nation has the obligation to segregate its military objectives from civilians and civilian objects. Second, for those military objectives that it cannot segregate, the nation has a responsibility to protect the civilians and civilian objects from the anticipated effects of attacks.

Importantly, those who wrote this provision of API discussed in some detail the difficulty of accomplishing this standard. The inclusion of the caveat “to the maximum extent feasible” was the basis of much discussion and was purposely added in a way to apply to the entire provision, meaning that both the segregate and protect requirements are limited by the feasibility of any required actions. 53 This is also reflected by the ICRC in the Commentary, which states that “it is clear that precautions should not go beyond the point where the life of the population would become difficult or even impossible.” 54

One more important point is worth noting before discussing the obligations in detail. The title of Article 58 specifically refers to “attacks”; however, Article 58(c) refers to “operations,” which cover a much broader spectrum of cyber activities. There is no doubt that the provisions discussed below, even those under the heading of “Protect,” apply to precautions against potential cyber attacks, but the extent to which these provisions apply to operations is unclear, particularly for State parties to API. For nations like the United States who are not parties and are only bound by this article to the extent that it reflects customary international law, it seems clear that the customary aspect of this rule applies only to “attacks” and not all operations. The news is replete with examples of attacks on military objectives that impact civilian infrastructure and systems, and no States appear to have accepted the obligation to protect these targets. 55
*213 A. Segregate

It is clear that this rule was originally written with a very "geographic" focus that is hard to translate to the cyber domain. Segregating a military armaments storage facility is geographically easier than segregating digital military communications. In fact, estimates of the U.S. Department of Defense digital traffic that traverses civilian-owned and operated infrastructure are between 90 and 98 percent.\(^{56}\) There is certainly still a geographic aspect to the rule, even in the cyber domain, but there is also a virtual location aspect to the provision.

The distinction between the virtual and geographic natures of this rule in its application to cyber operations is exemplified by the difference between cyber infrastructure and digital communications. A nation can comply with the geographic nature of the requirement by positioning servers and other military cyber equipment away from civilian areas. Similarly, a nation could conceivably create a separate cyber infrastructure backbone upon which its military cyber communications would traverse, effectively segregating it from civilian infrastructure. This has obviously not been the practice of States to this point.

Rather, the ubiquitous nature of the cyber domain has made it almost impossible to segregate potential military objectives from civilian objects even in a geographic sense. Consider air traffic control centers and other major civilian transportation control centers, as well as power generation facilities. All of these serve both civilian and military purposes and are clearly cyber targets, but they are also virtually impossible to segregate. State practice in this area has at least demonstrated that nations have not found such segregation to be feasible.

In fact, many militaries seem to be moving in the exact opposite direction and co-locating an ever greater percentage of their cyber infrastructure with civilian infrastructure. A good example of this is the movement of military and government data to the "cloud."\(^{57}\) While this move is heralded as providing great financial savings, it is unclear whether the legal obligation *214 of segregation of military objectives was ever considered as part of the decision to use the cloud.

**B. Protect**

Given the difficulty of segregating military objectives from civilians and civilian objects in the cyber domain, the subsequent duty to protect civilians and civilian objects from the indirect effects of attacks on nonsegregable military objectives becomes very important. The caveat of feasibility applies equally to this portion of the legal obligation, but the descriptive wording of "maximum extent" must also be allowed to have some meaning or the provision carries no legal weight at all.

1. "Dangers"

The requirement to protect does not encompass every potential cyber inconvenience or irritation. Rather, it applies only to "dangers" that might result from military operations. While this term is not defined in API, it seems reasonable to equate this standard to that used in the proportionality analysis discussed above, i.e., death or injury to civilians and damage to civilian objects.

Therefore, the protection obligation would not apply to cyber operations such as a denial of service attack that prevents access to a website or the altering of a website to change its appearance or connecting links. Instead, the obligation to protect should be understood to protect civilians and civilian objects from death or injury and destruction, such as shutting down air traffic control systems or power systems, which would result in serious effects on civilians.
2. “Under Their Control”

Another aspect of this rule that limits its general application is the use of the words “under their control.” The plain reading of the obligation makes it clear that governments are not expected to protect all civilians and civilian objects from the effects of attacks, but only those which fall under the government's control.

As with the general rule, this particular provision was originally conceived territorially. In the drafting debates, the Canadian representative, Brigadier General Wolfe, argued to change the originally proposed language *215 of “authority” to “control” to make clear the de facto nature of the obligation. 58 The change was accepted and the obligation amended. In the cyber context, the de facto nature of the rule has significant impact. A government might claim that it does not have authority over most of the cyber infrastructure due to the various legal regimes that exist within the nation. However, under the de facto standard, if the party can dictate the operations of a civilian computer system, it is under the control of that party and the duty to segregate or protect applies.

3. Specific Measures

The ICRC Commentary to Article 58 suggests examples of specific measures that a nation could take to fulfill its obligations under the rule, including providing well-trained civil defense forces, systems for warnings of impending attacks, and responsive fire and emergency services. 59 Analogizing these suggestions to the cyber world would suggest actions such as providing or requiring protective software products, monitoring networks and systems and providing warnings of impending or ongoing attacks, and providing technical assistance to repair networks or reroute them to alternative systems that continue to maintain functionality.

The U.S. government has already started to take some of these actions, though the extent to which it is taking them as a result of its legal obligation is unclear. For example, the United States has recently started the Defense Industrial Base Pilot Program, which is now expanding. 60 Under the program, specific industries providing defense services that make them legitimate targets in an armed conflict must meet certain cybersecurity requirements in order to do business with the government. Additionally, they receive some cyber assistance as a result of their membership in the program.

Additionally, the U.S. government recently stated that it will warn industries when they appear to be the target of an attack in an attempt to put *216 them on notice so they can increase their security posture. 61 Interestingly, the cyber giant Google has also recently announced that it will provide warnings to clients that appear to be the target of "State" hacking operations. 62 While Google certainly does not have any legal obligation under Article 58 to do so, it is interesting to note the sense that there is a need for such warnings.

Finally, the recent coordination between Google and the National Security Agency after the former was the victim of attacks from the Chinese government 63 may foreshadow an emerging cyber era where the government not only provides warning information, but then works closely to remediate and potentially retaliate for State-sponsored cyber activities that affect key civilian industries.

As a closing point to this part, it is important to note that a nation's inability or failure to fulfill its obligations under Article 58 does not affect an adversary's legal ability to conduct cyber attacks, so long as those attacks comply with the applicable rules of the LOAC.

VI. CONCLUSION

Cyber warfare is governed by the LOAC, and the LOAC does a generally good job of regulating cyber operations. In most cases, the existing law provides a clear paradigm to govern cyber activities; however, there are several areas where governments and military operators might question how to apply the LOAC to a specific cyber operation. This article has highlighted a few areas where additional clarity would be useful, such as in the cases of the definition of attack, the details of applying constant care, and *217 the required precautions against the effects of attacks. As the discussion on these issues increases, particularly spurred by the Tallinn Manual, and as State actions in cyberspace inevitably increase, State practice will provide nuance to the application of the LOAC that will allow clearer definition on the use of cyber operations in armed conflict.

Footnotes


6. The author was a member of the group.

7. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

8. The jus ad bellum regulates the laws of conflict management, or the laws governing going to war. The jus in bello regulates activities once armed conflict has begun. Though some terms are similar in both bodies of law, they are considered separate and distinct under the current armed conflict paradigm.


10. Id. at 34.


13 TALLINN MANUAL, supra note 7, rule 30.

14 For example, Michael Schmitt’s article on the application of these principles to non-international armed conflict discusses non-State actors. Michael Schmitt, *Classification of Cyber Conflict*, 89 INTERNATIONAL LAW STUDIES ___ (forthcoming 2013).


17 API, supra note 15, art. 57.1.

18 API COMMENTARY, supra note 16, at 680.


21 Sanger, supra note 1.

22 Nakashima, Miller & Tate, supra note 2.

23 Id.

24 For example, the Hague rules require the attacker to “do all in his power to warn the authorities” unless the attack is an “assault.” Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land art. 26, Oct. 18, 1907, 36 Stat. 2227, available at http://www.icrc.org/ihl.nsf/FULL/195?OpenDocument; see also TALLINN MANUAL, supra note 7, rule 58.


*See generally* TALLINN MANUAL, *supra* note 7, rule 51 (discussing the application of proportionality to cyber warfare).

API, *supra* note 15, art. 48.


WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 140 (1999) (where the author argues that "any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force that may constitute an armed attack prompting the right to self-defense"); TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 253-54 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) (which states "actions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage").


*Id.*


*Id.* (which states that "indirect effects of an attack may be one of the factors included when weighing anticipated incidental injury or death to protected persons").

Prosecutor v. Stanislav Galic, Case No. IT-98-29-T, Judgment, ¶ 58 (Int'l Crim. Trib. for the former Yugoslavia Dec. 5, 2003) (where the Trial Chamber held "[i]n determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack").


API, *supra* note 15, arts. 57.2(a)(i)-(ii), 58.

*Id.*, art. 57.4; API COMMENTARY, *supra* note 16, at 704; TALLINN MANUAL, *supra* note 7, sec. 7.

API, *supra* note 15, art. 57.2(a)(i).

*Id.*, art. 57.2(a)(ii).


6 *id.* at 214; Jensen, *supra* note 19, at 1548.
45 6 id. at 214; Jensen, supra note 19, at 1549.

46 Reservation Letter from Christopher Hulse, Ambassador from the United Kingdom to Switzerland, to the Swiss Government (Jan. 28, 1998), available at http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument (listing the United Kingdom's reservations and declarations to Additional Protocol I, and explaining in paragraph (b) that "[t]he United Kingdom understands the term 'feasible' as used in the Protocol to mean that which is practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations"). See also UK MANUAL, supra note 16, ¶ 5.32; ICRC CIL STUDY, supra note 16, at 54.

47 See United States v. Wilhelm List and others, XI Trials of War Criminals Before the Nuremberg Military Tribunals Under Control Council Law No. 10, at 1295 (1950) [hereinafter Hostage Judgment]; see also Jensen, supra note 26, at 1181-83.

48 Hostage Judgment, supra note 47, at 1296.

49 See generally TALLINN MANUAL, supra note 7, rule 59 (discussing precautions against the effects of attacks in relation to cyber operations).

50 API, supra note 15, art. 58.

51 ICRC CIL STUDY, supra note 16, at 68-69, 71, 74; NIAC MANUAL, supra note 16, ¶ 2.3.7; YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 145 (2d ed. 2010).

52 See generally Jensen, supra note 19.


54 API COMMENTARY, supra note 16, at 692.


56 See McConnell, supra note 19.


58 14 Official Records, supra note 43, at 198-99 (where it states, "[T]he use of the word 'control' would impose obligations on the parties which would not necessarily be implied by the use of the word 'authority.' It referred to the de facto as opposed to the de jure situation.").

59 API COMMENTARY, supra note 16, at 694-95; see also ICRC CIL STUDY, supra note 16, at 70.


Executive Order 12333
United States Intelligence Activities
(As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))

PREAMBLE

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended, (Act) and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1 Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts

1.1 Goals. The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests.

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:

(1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;

(2) Threats to the United States and its interests from terrorism; and

(3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 The National Security Council.

(a) Purpose. The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence,
counterintelligence, and covert action, and attendant policies and programs.

(b) **Covert Action and Other Sensitive Intelligence Operations.** The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 **Director of National Intelligence.** Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

1. Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

2. Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

1. Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived;

2. May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;

3. Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

4. In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

   (A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

   (B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

   (C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

5. Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence
programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:

(A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:

(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

(10) May, only with respect to Intelligence Community elements, and after consultation with the head of the originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.

(B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;
(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;
(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) Removal from certain positions.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head
chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

1.4 The Intelligence Community. Consistent with applicable Federal law and with the other provisions of this order, and under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;

(g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies. The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request, after consultation with the head of the department or agency, for the performance of the Director's functions;
(e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

1.6 Heads of Elements of the Intelligence Community. The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;

(f) Disseminate information or intelligence to foreign governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 Intelligence Community Elements. Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.
(a) THE CENTRAL INTELLIGENCE AGENCY. The Director of the Central Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;

(2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;

(2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;

(3) Conduct counterintelligence activities;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(l) of this order;

(6) Manage and coordinate all matters related to the Defense Attaché system; and

(7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;
(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and
(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.8 The Department of State. In addition to the authorities exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:

(a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;

(b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

(c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and

(d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 The Department of the Treasury. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 The Department of Defense. The Secretary of Defense shall:

(a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;
(b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in sections (a) through (i) above, and to support the Intelligence Community elements of the Department of Defense; and

(k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (l) and, when the Coast Guard is operating as part of the Department of Defense, above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 The Department of Homeland Security. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(l) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 The Department of Energy. In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(l) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;

(b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.
1.13 *The Federal Bureau of Investigation*. In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

**PART 2 Conduct of Intelligence Activities**

2.1 *Need.* Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 *Purpose.* This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 *Collection of information.* Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

480
In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 Collection Techniques. Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

1. Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

2. Searches by CIA of personal property of non-United States persons lawfully in its possession;

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

1. Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

2. Physical surveillance of a military person employed by a non-intelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 Assistance to Law Enforcement and other Civil Authorities. Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;

(b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;
(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 Contracting. Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 Consistency With Other Laws. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations Within the United States. No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person’s intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 Human Experimentation. No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject’s informed consent shall be documented as required by those guidelines.

2.11 Prohibition on Assassination. No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

2.12 Indirect Participation. No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 Limitation on Covert Action. No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 General Provisions

3.1 Congressional Oversight. The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be implemented in accordance with applicable law, including title V of the Act. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 Implementation. The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General’s approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.
3.3 Procedures. The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 References and Transition. References to "Senior Officials of the Intelligence Community" or "SOICs" in executive orders or other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 Definitions. For the purposes of this Order, the following terms shall have these meanings:

(a) **Counterintelligence** means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) **Covert action** means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

   (1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

   (2) Traditional diplomatic or military activities or routine support to such activities;

   (3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

   (4) Activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(c) **Electronic surveillance** means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) **Employee** means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) **Foreign intelligence** means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) **Intelligence** includes foreign intelligence and counterintelligence.

(g) **Intelligence activities** means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) **Intelligence Community** and elements of the Intelligence Community refers to:

   (1) The Office of the Director of National Intelligence;

   (2) The Central Intelligence Agency;

   (3) The National Security Agency;

   (4) The Defense Intelligence Agency;

   (5) The National Geospatial-Intelligence Agency;

   (6) The National Reconnaissance Office;
(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) National Intelligence and Intelligence Related to National Security means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(j) The National Intelligence Program means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) United States person means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 Revocation. Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

3.7 General Provisions.

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

(1) Authority granted by law to a department or agency, or the head thereof; or

(2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.
NATIONAL INSIDER THREAT POLICY

The National Insider Threat Policy aims to strengthen the protection and safeguarding of classified information by: establishing common expectations; institutionalizing executive branch best practices; and enabling flexible implementation across the executive branch.

A. Policy

Executive Order 13587 directs United States Government executive branch departments and agencies (departments and agencies) to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect classified national security information (as defined in Executive Order 13526; hereinafter classified information), and requires the development of an executive branch program for the deterrence, detection, and mitigation of insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. Executive Order 12968 promulgates classified information access eligibility policy and establishes a uniform Federal personnel security program for employees considered for initial or continued access to classified information. Consistent with Executive Orders 13587 and 12968, this policy is applicable to all executive branch departments and agencies with access to classified information, or that operate or access classified computer networks; all employees with access to classified information, including classified computer networks (and including contractors and others who access classified information, or operate or access classified computer networks controlled by the federal government); and all classified information on those networks.

This policy leverages existing federal laws, statutes, authorities, policies, programs, systems, architectures and resources in order to counter the threat of those insiders who may use their authorized access to compromise classified information. Insider threat programs shall employ risk management principles, tailored to meet the distinct needs, mission, and systems of individual agencies, and shall include appropriate protections for privacy, civil rights, and civil liberties.

B. General Responsibilities of Departments and Agencies

1) Within 180 days of the effective date of this policy, establish a program for deterring, detecting, and mitigating insider threat; leveraging counterintelligence (CI), security, information assurance, and other relevant functions and resources to identify and counter the insider threat.

2) Establish an integrated capability to monitor and audit information for insider threat detection and mitigation. Critical program requirements include but are not limited to: (1) monitoring user activity on classified computer networks controlled by the Federal Government; (2) evaluation of personnel security information; (3) employee awareness training of the insider threat and employees' reporting responsibilities; and (4) gathering information for a centralized analysis, reporting, and response capability.

3) Develop and implement sharing policies and procedures whereby the organization’s insider threat program accesses, shares, and integrates information and data derived from
offices across the organization, including CI, security, information assurance, and human resources offices.

4) Designate a senior official(s) with authority to provide management, accountability, and oversight of the organization’s insider threat program and make resource recommendations to the appropriate agency official.

5) Consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, civil liberties issues (including use of personally identifiable information) are appropriately addressed.

6) Promulgate additional department and agency guidance, if needed, to reflect unique mission requirements, but not inhibit meeting the minimum standards issued by the Insider Threat Task Force (ITTF) pursuant to this policy.

7) Perform self-assessments of compliance with insider threat policies and standards; the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee (hereinafter Steering Committee).

8) Enable independent assessments, in accordance with Section 2.1(d) of Executive Order 13587, of compliance with established insider threat policy and standards by providing information and access to personnel of the ITTF.

C. Insider Threat Task Force roles and responsibilities

The ITTF, established under Executive Order 13587, is the principal interagency task force responsible for developing an executive branch insider threat detection and prevention program to be implemented by all departments and agencies covered by this policy. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within departments and agencies.

The ITTF shall:

1) In coordination with appropriate agencies, develop and issue minimum standards and guidance for implementing insider threat program capabilities throughout the executive branch. These standards shall include, but are not limited to, the following:
   • Monitoring of user activity on United States Government networks. This refers to audit data collection strategies for insider threat detection, leveraging hardware and/or software with triggers deployed on classified networks to detect, monitor, and analyze anomalous user behavior for indicators of misuse.
   • Continued evaluation of personnel security information whereby information is gathered from, including but not limited to, an individual’s security background investigation, clearance adjudication, foreign travel reporting, foreign contact reporting, financial disclosure, polygraph examination results (where applicable) or other personnel actions, and made available to authorized insider threat program personnel to assess, in conjunction with anomalous user behavior data, and/or any other insider threat concern or allegation.
   • Employee awareness training of the insider threat, the inherent risk posed to classified information by malicious insiders and, specifically, recognition of insider threat behaviors; developing a reporting structure to ensure all employees and contractors
report suspected insider threat activity consistently and securely; informing employees, subject to monitoring, of the policies and processes in place to protect their privacy, civil rights, and civil liberties rights against unnecessary monitoring (to include retaliation against whistleblowers); and, ensuring employee awareness of their responsibility to report, as well as how and to whom to report, suspected insider threat activity.

- Analysis, Reporting and Response: gathering and integrating available information to conduct a preliminary review of any potential insider threat issues; and, where it appears a potential threat may exist, taking action by referring the matter as appropriate to CI, security, information assurance, the Office of Inspector General, or to the proper law enforcement authority.

2) Review and update ITTF standards and guidance, as appropriate.

3) Provide continual assistance to departments and agencies to establish and/or improve insider threat detection and prevention programs. The nature of assistance will involve a collaborative process wherein subject matter expert(s) provide expertise, guidance, and advice through various forums including on site visits.

4) Conduct independent assessments at individual organizations, as directed by the Steering Committee and in coordination with Executive Agent for Safeguarding (EA/S) and the Classified Information Sharing and Safeguarding Office (CISSO) established by Executive Order 13587, to determine the level of organizational compliance with this policy and minimum insider threat standards.

5) Use the results of relevant insider threat data sources to include, but not limited to, the agency’s Key Information Sharing and Safeguarding Indicators self-assessments, applicable portions of the Office of the National Counterintelligence Executive Mission Reviews and Program Assessments, and the results of assistance visits and independent assessments to determine the adequacy of insider threat programs at individual agencies, and Government-wide.

6) Coordinate with the Information Security Oversight Office (ISOO), EA/S, and the CISSO to report results of independent assessments to the Steering Committee for use in the annual reports submitted to the President assessing the executive branch’s effectiveness in implementing insider threat programs, and to inform related program and budget recommendations.

7) Refer to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards.

8) Provide strategic analysis of new and continuing insider threat challenges facing the United States Government.

D. Definitions

Classified information: Information that has been determined pursuant to Executive Order 13526, or any successor order, Executive Order 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and that is marked to indicate its classified status when in documentary form.

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations
conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. (Executive Order 12333, as amended)


Employee: For purposes of this policy, “employee” has the meaning provided in section 1.1(e) of Executive Order 12968; specifically: a person, other than the President and Vice President, employed by, detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Insider: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

Insider Threat: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Key Information Sharing and Safeguarding Indicators: The Steering Committee developed these key performance indicators to serve as the basis for addressing reporting requirements directed by the President, and to assist in tracking progress and identifying areas for attention or additional funding to continue and strengthen the sharing and safeguarding of classified information on computer networks.

E. General Provisions

Nothing in this policy shall be construed to supersede or change the requirements of the National Security Act of 1947, as amended; the Atomic Energy Act of 1954, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order 12333, as amended (2008); Executive Order 13467, (2008); Executive Order 13526, (2009); Executive Order 12829, as amended, (1993); Executive Order 13549 (2010); and Executive Order 12968, (1995) and their successor orders or directives.
MINIMUM STANDARDS FOR EXECUTIVE BRANCH INSIDER THREAT PROGRAMS


B. PURPOSE

1. Executive Order 13587 establishes the Insider Threat Task Force, co-chaired by the Director of National Intelligence and the Attorney General, and requires, in coordination with appropriate agencies, the development of minimum standards and guidance for implementation of a government-wide insider threat policy. This policy provides those minimum requirements and guidance for executive branch insider threat detection and prevention programs.

2. Insider threat programs are intended to: deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative or other response actions as outlined in Section E.2.

3. The standards herein shall serve as minimum requirements for all applicable executive branch agencies. Nothing in this document shall be construed to supersede existing or future Intelligence Community or Department of Defense policy, which may impose more stringent requirements beyond these minimum standards for insider threat programs. Agencies may establish additional standards, provided that they are not inconsistent with the requirements contained herein.

4. Agency heads are ultimately responsible for the establishment and operations of their respective insider threat programs. Designated senior official(s), as described in Section D, shall be responsible for implementing the minimum standards contained herein.

C. APPLICABILITY: These standards shall apply to any “executive agency,” as defined in 5 U.S.C. §105; any “military department” as defined in 5 U.S.C. §102; any “independent establishment” as defined in 5 U.S.C. §104(1); any intelligence community element as defined in Executive Order 12333.

D. DESIGNATION OF SENIOR OFFICIAL(S): Each agency head shall designate a senior official or officials, who shall be principally responsible for establishing a process to gather, integrate, and centrally analyze, and respond to Counterintelligence (CI), Security, Information Assurance (IA), Human Resources (HR), Law Enforcement (LE), and other relevant information indicative of a potential insider threat. Senior Official(s) shall:

1. Provide management and oversight of the insider threat program and provide resource recommendations to the agency head.

2. Develop and promulgate a comprehensive agency insider threat policy to be approved by the agency head within 180 days of the effective date of the National Insider Threat Policy. Agency policies shall include internal guidelines and procedures for the implementation of the standards contained herein.

3. Submit to the agency head an implementation plan for establishing an insider threat program and annually thereafter a report regarding progress and/or status within that agency. At a
minimum, the annual reports shall document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges.

4. Ensure the agency's insider threat program is developed and implemented in consultation with that agency's Office of General Counsel and civil liberties and privacy officials so that all insider threat program activities to include training are conducted in accordance with applicable laws, whistleblower protections, and civil liberties and privacy policies.

5. Establish oversight mechanisms or procedures to ensure proper handling and use of records and data described below, and ensure that access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions.

6. Ensure the establishment of guidelines and procedures for the retention of records and documents necessary to complete assessments required by Executive Order 13587.

7. Facilitate oversight reviews by cleared officials designated by the agency head to ensure compliance with insider threat policy guidelines, as well as applicable legal, privacy and civil liberty protections.

E. INFORMATION INTEGRATION, ANALYSIS AND RESPONSE: Agency heads shall:

1. Build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess, and respond to information derived from CI, Security, IA, HR, LE, the monitoring of user activity, and other sources as necessary and appropriate.

2. Establish procedures for insider threat response action(s), such as inquiries, to clarify or resolve insider threat matters while ensuring that such response action(s) are centrally managed by the insider threat program within the agency or one of its subordinate entities.

3. Develop guidelines and procedures for documenting each insider threat matter reported and response action(s) taken, and ensure the timely resolution of each matter.

F. INSIDER THREAT PROGRAM PERSONNEL: Agency heads shall ensure personnel assigned to the insider threat program are fully trained in:

1. Counterintelligence and security fundamentals to include applicable legal issues;

2. Agency procedures for conducting insider threat response action(s);

3. Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information;

4. Applicable civil liberties and privacy laws, regulations, and policies; and

5. Investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995, as well as other policy or statutory requirements that require referrals to an internal
entity, such as a security office or Office of Inspector General, or external investigative entities such as the Federal Bureau of Investigation, the Department of Justice, or military investigative services.

G. ACCESS TO INFORMATION: Agency heads shall:

1. Direct CI, Security, IA, HR, and other relevant organizational components to securely provide insider threat program personnel regular, timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. Such access and information includes, but is not limited to, the following:

   a. Counterintelligence and Security. All relevant databases and files to include, but not limited to, personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings.

   b. Information Assurance. All relevant unclassified and classified network information generated by IA elements to include, but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.

   c. Human Resources. All relevant HR databases and files to include, but not limited to, personnel files, payroll and voucher files, outside work and activities requests disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

2. Establish procedures for access requests by the insider threat program involving particularly sensitive or protected information, such as information held by special access, law enforcement, inspector general, or other investigative sources or programs, which may require that access be obtained upon request of the Senior Official(s).

3. Establish reporting guidelines for CI, Security, IA, HR, and other relevant organizational components to refer relevant insider threat information directly to the insider threat program.

4. Ensure insider threat programs have timely access, as otherwise permitted, to available United States Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.

H. MONITORING USER ACTIVITY ON NETWORKS: Agency heads shall ensure insider threat programs include:

1. Either internally or via agreement with external agencies, the technical capability, subject to appropriate approvals, to monitor user activity on all classified networks in order to detect activity indicative of insider threat behavior. When necessary, Service Level Agreements (SLAs) shall be executed with all other agencies that operate or provide classified network connectivity or systems. SLAs shall outline the capabilities the provider will employ to identify suspicious user behavior and how that information shall be reported to the subscriber’s insider threat personnel.
2. Policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.

3. Agreements signed by all cleared employees acknowledging that their activity on any agency classified or unclassified network, to include portable electronic devices, is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding. Agreement language shall be approved by the Senior Official(s) in consultation with legal counsel.

4. Classified and unclassified network banners informing users that their activity on the network is being monitored for lawful United States Government-authorized purposes and can result in criminal or administrative actions against the user. Banner language shall be approved by the Senior Official(s) in consultation with legal counsel.

I. EMPLOYEE TRAINING AND AWARENESS: Agency heads shall ensure insider threat programs:

1. Provide insider threat awareness training, either in-person or computer-based, to all cleared employees within 30 days of initial employment, entry-on-duty (EOD), or following the granting of access to classified information, and annually thereafter. Training shall address current and potential threats in the work and personal environment, and shall include, at a minimum, the following topics:
   a. The importance of detecting potential insider threats by cleared employees and reporting suspected activity to insider threat personnel or other designated officials;
   b. Methodologies of adversaries to recruit trusted insiders and collect classified information;
   c. Indicators of insider threat behavior and procedures to report such behavior; and
   d. Counterintelligence and security reporting requirements, as applicable.

2. Verify that all cleared employees have completed the required insider threat awareness training contained in these standards.

3. Establish and promote an internal network site accessible to all cleared employees to provide insider threat reference material, including indicators of insider threat behavior, applicable reporting requirements and procedures, and provide a secure electronic means of reporting matters to the insider threat program.

J. DEFINITIONS

"Agency Head" means the head of any: "executive agency," as defined in 5 U.S.C. §105; "military department" as defined in 5 U.S.C. §102; "independent establishment" as defined in 5 U.S.C. §104; intelligence community element as defined in Executive Order 12333; and any other entity within the executive branch that comes into the possession of classified information.

"Classified Information" means information that has been determined pursuant to Executive Order 13526, or the Atomic Energy Act of 1954 (42 U.S.C. §2162), to require
protection against unauthorized disclosure and that it is marked to indicate its classified status when in documentary form.

“Cleared Employee” means a person who has been granted access to classified information, other than the President and Vice President, employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

“Insider Threat” means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

“Insider Threat Response Action(s)” means activities to ascertain whether certain matters or information indicates the presence of an insider threat, as well as activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of CI, Security, LE, or IG elements depending on statutory authority and internal policies governing the conduct of such in each agency.

“Subordinate Entity” means an office, command, or similar organization, subordinate to the agency, which manages its own insider threat program.
Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.
(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency’s activities.
(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to
the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.
(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the
Federal Acquisition Regulatory Council, shall make recommendations to the
President, through the Assistant to the President for Homeland Security and
Counterterrorism and the Assistant to the President for Economic Affairs, on
the feasibility, security benefits, and relative merits of incorporating security
standards into acquisition planning and contract administration. The report
shall address what steps can be taken to harmonize and make consistent
existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150
days of the date of this order, the Secretary shall use a risk-based approach to
identify critical infrastructure where a cybersecurity incident could reasonably
result in catastrophic regional or national effects on public health or safety,
economic security, or national security. In identifying critical infrastructure for
this purpose, the Secretary shall use the consultative process established in
section 6 of this order and draw upon the expertise of Sector-Specific
Agenices. The Secretary shall apply consistent, objective criteria in identifying
such critical infrastructure. The Secretary shall not identify any commercial
information technology products or consumer information technology services
under this section. The Secretary shall review and update the list of identified
critical infrastructure under this section on an annual basis, and provide such
list to the President, through the Assistant to the President for Homeland
Security and Counterterrorism and the Assistant to the President for Economic
Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall
provide the Secretary with information necessary to carry out the
responsibilities under this section. The Secretary shall develop a process for
other relevant stakeholders to submit information to assist in making the
identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall
confidentially notify owners and operators of critical infrastructure identified
under subsection (a) of this section that they have been so identified, and
ensure identified owners and operators are provided the basis for the
determination. The Secretary shall establish a process through which owners
and operators of critical infrastructure may submit relevant information and
request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating
the security of critical infrastructure shall engage in a consultative process
with DHS, OMB, and the National Security Staff to review the preliminary
Cybersecurity Framework and determine if current cybersecurity regulatory
requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be

independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive-21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.
(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA
Executive Order -- Promoting Private Sector Cybersecurity Information Sharing

EXECUTIVE ORDER

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-I (PPD-I) of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 2. Information Sharing and Analysis Organizations. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.
Sec. 3. ISAO Standards Organization. (a) The Secretary, in consultation with other Federal entities responsible for conducting cybersecurity and related activities, shall, through an open and competitive process, enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order. The standards shall further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information. The standards will address the baseline capabilities that ISAOs under this order should possess and be able to demonstrate. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical means, and privacy protections, such as minimization, for ISAO operation and ISAO member participation.

(b) To be selected, the SO must demonstrate the ability to engage and work across the broad community of organizations engaged in sharing information related to cybersecurity risks and incidents, including ISAOs, and associations and private companies engaged in information sharing in support of their customers.

(c) The agreement referenced in section 3(a) shall require that the SO engage in an open public review and comment process for the development of the standards referenced above, soliciting the viewpoints of existing entities engaged in sharing information related to cybersecurity risks and incidents, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders.

(d) The Secretary shall support the development of these standards and, in carrying out the requirements set forth in this section, shall consult with the Office of Management and Budget, the National Institute of Standards and Technology in the Department of Commerce, Department of Justice, the Information Security Oversight Office in the National Archives and Records Administration, the Office of the Director of National Intelligence, Sector-Specific Agencies, and other interested Federal entities. All standards shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

Sec. 4. Critical Infrastructure Protection Program. (a) Pursuant to sections 213 and 214(h) of the Critical Infrastructure Information Act of 2002, I hereby designate the NCCIC as a critical infrastructure protection program and delegate to it authority to enter into voluntary agreements with ISAOs in order to promote critical infrastructure security with respect to cybersecurity.

(b) Other Federal entities responsible for conducting cybersecurity and related activities to address threats to the public health and safety, national security, and economic security, consistent with the objectives of this order, may participate in activities under these agreements.

(c) The Secretary will determine the eligibility of ISAOs and their members for any necessary facility or personnel security clearances associated with voluntary agreements in accordance with Executive Order 13549 of August 18, 2010 (Classified National Security Information Programs for State, Local, Tribal, and
Private Sector Entities), and Executive Order 12829 of January 6, 1993 (National Industrial Security Program), as amended, including as amended by this order.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that appropriate protections for privacy and civil liberties are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency’s activities.

(b) Senior privacy and civil liberties officials for agencies engaged in activities under this order shall conduct assessments of their agency’s activities and provide those assessments to the Department of Homeland Security (DHS) Chief Privacy Officer and the DHS Office for Civil Rights and Civil Liberties for consideration and inclusion in the Privacy and Civil Liberties Assessment report required under Executive Order 13636.

Sec. 6. National Industrial Security Program. Executive Order 12829, as amended, is hereby further amended as follows:

(a) the second paragraph is amended by inserting “the Intelligence Reform and Terrorism Prevention Act of 2004,” after “the National Security Act of 1947, as amended,”;

(b) Sec. 101(b) is amended to read as follows: “The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order 13526 of December 29, 2009, or any predecessor or successor order, and the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).”;

(c) Sec. 102(b) is amended by replacing the first paragraph with: “In consultation with the National Security Advisor, the Director of the Information Security Oversight Office, in accordance with Executive Order 13526 of December 29, 2009, shall be responsible for implementing and monitoring the National Industrial Security Program and shall:”;

(d) Sec. 102(c) is amended to read as follows: “Nothing in this order shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.), or the authority of the Director of National Intelligence (or any Intelligence Community element) under the Intelligence Reform and Terrorism Prevention Act of 2004, the National Security Act of 1947, as amended, or Executive Order 12333 of December 8, 1981, as amended, or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities).”;

(e) Sec. 201(a) is amended to read as follows: “The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, the Director of National Intelligence, and the Secretary of Homeland Security, shall issue and maintain a National Industrial Security Program Operating Manual (Manual). The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under


508
the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.). The Director of National Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information. The Secretary of Homeland Security shall prescribe and issue that portion of the Manual that pertains to classified information shared under a designated critical infrastructure protection program.

(f) Sec. 201(f) is deleted in its entirety;

(g) Sec. 201(e) is redesignated Sec. 201(f) and revised by substituting "Executive Order 13526 of December 29, 2009, or any successor order," for "Executive Order No. 12356 of April 2, 1982.";

(h) Sec. 201(d) is redesignated Sec. 201(e) and revised by substituting "the Director of National Intelligence, and the Secretary of Homeland Security" for "and the Director of Central Intelligence."

(i) a new Sec. 201(d) is inserted after Sec. 201(c) to read as follows: "The Manual shall also prescribe arrangements necessary to permit and enable secure sharing of classified information under a designated critical infrastructure protection program to such authorized individuals and organizations as determined by the Secretary of Homeland Security."

(j) Sec. 202(b) is amended to read as follows: "The Director of National Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of National Intelligence may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, or with the Director of the Central Intelligence Agency to inspect and monitor these programs or facilities, in whole or in part, on the Director's behalf."

(k) Sec. 202(d) is redesignated as Sec. 202(e); and

(l) in Sec. 202 a new subsection (d) is inserted after subsection (c) to read as follows: "The Secretary of Homeland Security may determine the eligibility for access to Classified National Security Information of contractors, licensees, and grantees and their respective employees under a designated critical infrastructure protection program, including parties to agreements with such program; the Secretary of Homeland Security may inspect and monitor contractor, licensee, and grantee programs and facilities or may enter into written agreements with the Secretary of Defense, as Executive Agent, or with the Director of the Central Intelligence Agency, to inspect and monitor these programs or facilities in whole or in part, on behalf of the Secretary of Homeland Security."

Sec. 7. Definitions. (a) "Critical infrastructure information" has the meaning given the term in section 212(3) of the Critical Infrastructure Information Act of 2002.

(b) "Critical infrastructure protection program" has the meaning given the term in section 212(4) of the Critical Infrastructure Information Act of 2002.
(c) "Cybersecurity risk" has the meaning given the term in section 226(a)(1) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(d) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(e) "Incident" has the meaning given the term in section 226(a)(2) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(f) "Information Sharing and Analysis Organization" has the meaning given the term in section 212(S) of the Critical Infrastructure Information Act of 2002.

(g) "Sector-Specific Agency" has the meaning given the term in PPD-21, or any successor.

Sec. 8. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law or Executive Order to an agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law including those activities conducted with the private sector relating to criminal and national security threats. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA
Executive Order 13694 of April 1, 2015

Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, BARACK OBAMA, President of the United States of America, find that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat.

Accordingly, I hereby order:

Section 1. (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in:

(i) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of:

(A) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(C) causing a significant disruption to the availability of a computer or network of computers; or

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or

(ii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State:

(A) to be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States;
(B) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity described in subsections (a)(i) or (a)(ii)(A) of this section or any person whose property and interests in property are blocked pursuant to this order;

(C) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order; or

(D) to have attempted to engage in any of the activities described in subsections (a)(i) and (a)(ii)(A)–(C) of this section.

(b) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of this order.

Sec. 2. I hereby determine that the making of donations of the type of articles specified in section 203(b)(2) of IEEPA (50 U.S.C. 1702(b)(2)) by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to section 1 of this order would seriously impair my ability to deal with the national emergency declared in this order, and I hereby prohibit such donations as provided by section 1 of this order.

Sec. 3. The prohibitions in section 1 of this order include but are not limited to:

(a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order; and

(b) the receipt of any contribution or provision of funds, goods, or services from any such person.

Sec. 4. I hereby find that the unrestricted immigrant and nonimmigrant entry into the United States of aliens determined to meet one or more of the criteria in section 1(a) of this order would be detrimental to the interests of the United States, and I hereby suspend entry into the United States, as immigrants or nonimmigrants, of such persons. Such persons shall be treated as persons covered by section 1 of Proclamation 8693 of July 24, 2011 (Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions).

Sec. 5. (a) Any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order is prohibited.

(b) Any conspiracy formed to violate any of the prohibitions set forth in this order is prohibited.

Sec. 6. For the purposes of this order:

(a) the term “person” means an individual or entity;

(b) the term “entity” means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(c) the term “United States person” means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States;

(d) the term “critical infrastructure sector” means any of the designated critical infrastructure sectors identified in Presidential Policy Directive 21; and

(e) the term “misappropriation” includes any taking or obtaining by improper means, without permission or consent, or under false pretenses.

Sec. 7. For those persons whose property and interests in property are blocked pursuant to this order who might have a constitutional presence
in the United States, I find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in this order, there need be no prior notice of a listing or determination made pursuant to section 1 of this order.

Sec. 8. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of this order. The Secretary of the Treasury may redelegate any of these functions to other officers and agencies of the United States Government consistent with applicable law. All agencies of the United States Government are hereby directed to take all appropriate measures within their authority to carry out the provisions of this order.

Sec. 9. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to submit the recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 10. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
April 1, 2015.
CHAPTER 18: LEGAL

American Bar Association Cybersecurity Legal Task Force

Harvey Rishikof, Co-Chair and Special Advisor for the Standing Committee on National Security, USA

Conor Sullivan, Law Clerk for the Standing Committee on National Security, USA

It is beneficial to spend some time understanding the legal paradigms which drive cyber law today. For our purposes, it is worth examining the legal frameworks in the two places modern organizations are perhaps the most likely to do business subject to cyber regulations: the European Union (E.U.) and United States (U.S.). Before doing so, let us overview how the ‘regulatory dots’ are connected as in TABLE 18.1.

EUROPEAN UNION (EU) AND INTERNATIONAL REGULATORY SCHEMES

The European Union

The European Union will soon be establishing a unified cyber law system beyond the 1995 E.U. Data Protection Directive.¹ The current E.U. Data Protection Directive was enacted in 1995, and was the original effort at determining data regulations within the E.U.² In this directive, the processing of personal data – data which could be used to identify an individual – must be transparent, have a legitimate purpose, used in a means proportional to the reason the data was

v4 August 31, 2016

initially collected, and provide some information to the subject about their retained rights to the data.\(^3\)

The upcoming application of the General Data Protection Regulation (GDPR) builds on these protections for personal data, placing further obligations on data processors – notably to create a Data Protection Officer (DPO), creating a lead supervisory authority for E.U. cyber regulations, creating a “right to erasure” and increasing the requirements for consumer consent to data collection.\(^4\) These impost are placed on the organization processing or controlling the data to the extent it happens within the E.U., or regardless of where the processing takes place - as long as the data processed is related to goods or services offered within the E.U.\(^5\) The GDPR also known as ‘EU Regulations (EU) 2016/679’ has been passed by the European Parliament, but will not be phased in until 25 May 2018.\(^6\)

**Transfer of data out of the EU, including the U.S.**

The GDPR also updates the 1995 Data Protection Directive’s limitations on the transfer of personal data to countries outside of the E.U., further defining what determines that a country provides “adequate protection” of the data to avoid ancillary agreements.\(^7\) The U.S. has negotiated an exception to this rule in the “E.U. – U.S. Privacy Shield” which will come into effect August 2016.\(^8\) The “Privacy Shield” will provide companies which transfer data across the Atlantic with a clear set of legal standards and protections surrounding consumer data which must be followed to participate in commerce with the E.U. U.S. corporations will be subject to compliance review with the U.S. Department of Commerce, as well as redress mechanisms set up to ensure that access to the data by government agencies will be as limited as possible.\(^9\)

An auxiliary bill working its way through the E.U. government is the Network and Information Security Directive (NISD). It has similarities to the GDPR by way of its broad footing but mainly concerns nations and critical infrastructure (CI).\(^10\) Under NISD, countries are to designate cyber response contact points in their governments and specific companies as “operators of essential services”, while the selected companies have expanded cybersecurity expectations and an incident notification requirements.\(^11\)

**Post - “Brexit” United Kingdom (UK)**

In regards to the United Kingdom’s (U.K.‘s) planned withdrawal from the E.U., in all likelihood the U.K. will continue to abide by E.U. privacy laws until the exact moment the union is broken, but there is little beyond conjecture to determine what would happen post - “Brexit”.\(^12\) Assuming

---

\(^3\) Ibid, Art 3.
\(^5\) Ibid.
\(^6\) Ibid.
\(^11\) Ibid.
\(^12\) https://www.crowelldatalaw.com/2016/06/privacy-cybersecurity-weekly-news-update-11/
that there is no “adequacy decision” immediately available from the European Commission when the U.K. exits – determining that the U.K.’s cyber laws are strong enough to be compliant with the E.U. policies – companies would have to implement “standard contractual clauses” or “binding corporate rules” to transfer data from the E.U. to U.K. immediately after the exit.\textsuperscript{13}

These clauses are approved by the E.U. government as sufficient to provide adequate safeguards to the privacy and data rights of E.U. citizens.\textsuperscript{14}

\textbf{International Organization for Standardization (ISO)}

The International Organization for Standardization (ISO) is an international non-governmental organization dedicated to setting international standards for organization activity. ISO 27001 and 27002 encompass the ISO’s take on managing information security risks, providing a method to identify risks, plan to address them, and implement controls. 27001 is organized in a “plan-do-check-act” manner similar to other ISO programs, making interaction with other ISO programs, such as ISO 22301 for Business Continuity management systems, possible – if not encouraged. While compliance with ISO standards are not outright required by regulations, the close relationship between cybersecurity methods, risk management, and organization planning makes ISO’s organizational offerings across multiple perspectives potentially advantageous.

\textbf{UNITED STATES (U.S.) REGULATIONS}

\textbf{Post-9/11 United States (U.S.)}

The U.S. national security paradigm has changed massively since the “age of innocence” pre-September 11. If that time of innocence is termed as “Security 1.0,” the world now anxiously sits in “Security 3.0” awaiting the emergence of “Security 4.0.”

The events of 9/11 led to the quick enactment of “Security 2.0” where regulations prioritized physical security and critical infrastructure security, but cybersecurity was still largely focused on preventing mischievous hackers more than malicious disruption of critical infrastructure.

“Security 3.0” defines the modern world as we know it where there is recognition of the importance data plays to the world and there are some regulations to protect personal information, but what overall role the government should play in ensuring cybersecurity is still in flux. Threats from criminals, hackers, espionage and potentially the military in a time of war has created a volatile space. Creating a single common cybersecurity framework has been challenging when faced with questions of federalism, agency politicking, and technological advancement.

Finally, “Security 4.0” seems to be emerging from an increasingly interconnected world – driven by a “big data” economy and the increasing “internet of things.” In this era, regulators and organizations will have to focus more on proactive prevention of cyber events rather than reactions, and not just for organizations within their nation – but for organizations which span

\textsuperscript{13} ibid.

\textsuperscript{14} http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm;
the world. "Security 4.0" presents new, monumental challenges to the existing national security paradigms which will only be addressed with time.

Cybersecurity negligence remains unclear

One method to avoid traditional negligence liability in a U.S. court is by proving that the standard of care – set by the legislature or judicial precedent – has been met. But there has been as of yet, no clear, defined standard of care set in the question of cybersecurity negligence.\(^{15}\) Instead, a patchwork of state, federal, and international laws and regulations have combined to form a rough guideline: steps to secure data must be “reasonable” or “appropriate” – taking the relevant circumstances into account – in order to avoid liability.\(^{16}\) To satisfy this requirement of reasonableness, a company should use a risk assessment process and craft a cybersecurity plan based off the findings.\(^{17}\)

Until recently, there was little guidance beyond industry report recommendations on what sort of process or measures were enough to be "reasonable" for companies in industries without specific cyber regulations.\(^{18}\) Currently, the U.S. private sector has been gravitating towards the U.S. National Institute of Standards and Technology’s (NIST’s) published cyber framework. NIST was originally given the responsibility to create the framework by Executive Order 13636, but the responsibility was then codified by the Cybersecurity Enhancement Act of 2014.

Adapting to the NIST framework is currently voluntary for non-critical infrastructure (CI) companies, but company partnerships between non-NIST compliant companies and CI are restricted – driving further adoption of the NIST standards throughout the economy. A similar scheme is rapidly being implemented within the federal contracting industry, requiring contractors to adopt specific data security standards to remain competitive for government contracts. As a result, more public-private business transactions are voluntarily becoming dependent on both parties having a NIST satisfactory level of cybersecurity. (Ed. note: Our Chapter 7 surveys standards and frameworks and contains a detailed section on NIST).

Specific U.S. industry/sector regulations

While general laws on cybersecurity are sparse in the U.S., some specific industries are highly regulated. As mentioned previously, Critical Infrastructure (CI) organizations must abide by the NIST framework as well as cooperate with the Department of Homeland Security, the Cyber Threat Intelligence Integration Center, and law enforcement with regards to cyber incident reporting and response.

The telecommunications sector is voluntarily covered by the NIST framework, and is encouraged to hold regular meetings between the FCC and individual companies to discuss cyber programs for risk management.

Energy producers have similarly been put on the NIST framework from the Department of Energy’s Cybersecurity Framework Implementation Guidance and our regulated by specific regulatory bodies, such as the Federal Energy Regulatory Commission.

\(^{15}\) http://www.tlij.org/content/journal/50/14%20SHACKELFORD%20PUB%20PROOF.pdf p.11

\(^{16}\) Rishikof, H. and George, H. A Playbook for Cyber Events, ABA Press, 2014, pp 39-42

\(^{17}\) Ibid p.49

\(^{18}\) http://www.tlij.org/content/journal/50/14%20SHACKELFORD%20PUB%20PROOF.pdf p.13
For government contractors, there has been a similar strengthening of cyber rules. In August 2015, the Department of Defense (DOD) released for the Defense Industrial Base (DIB) a revised version of the “Safeguarding Rule” – which requires companies contracting with DOD to implement a more expansive set of security controls.

Many other federal agencies are considering similar rules, with the Office of Management and Budget considering a comparable rule to apply to all contractors.

Financial services have had significant past regulation in regards to cyber, requiring compliance with rules set down by the Federal Financial Institution Examination Council on behalf of a slew of Federal Regulatory agencies. Companies which deal in securities and futures have been similarly regulated to necessitate the adoption of an Information System Security Program (ISSP). The ISSP must meet certain generally accepted standards or risk censure by regulating organizations, pushing more industries into adopting the NIST framework. The Securities and Exchange Commission (SEC) has signaled an increased emphasis on advisers having adequate cyber policy, rather than on responses to a breach and the harm suffered by the client. The Financial Industry Regulatory Authority (FINRA) has also created a report on cybersecurity best practices, pertaining to cybersecurity planning for broker-dealers.

The healthcare industry must abide by a series of regulations under the Health Insurance Portability and Accountability Act (HIPAA), which were split into a “Privacy Rule” and “Security Rule.” The Privacy Rule establishes standards for the protection of certain personal health information. The “Security Rule” acts on the protections laid out by the “Privacy Rule” by addressing “technical and non-technical safeguards that organizations called ‘covered entities’ must put in place to secure individuals’ ‘electronic protected health information’ (e-PHI).” The “Security Rule” seeks to ensure the protection of personal health information while allowing new technologies to improve patient care.

The previous examples are just a selection of some industries with specific regulatory schemes already being developed. Tom would be well served by asking his legal counsel to compile a more comprehensive list of regulations which pertain to his specific industry, simply to ensure that if regulations or guidelines exist – they are either being met or are being addressed in upcoming plans.

General fiduciary duty in the U.S.

The FTC has brought several regulatory actions against companies for failing to prevent unauthorized access to consumer information as “unfair or deceptive acts”. The settlements from these cases can involve increased information security requirements or long running independent audit schemes. There are also state and federal laws which support private actions against companies for unfair and deceptive trade practices, data breach notification, and failure

---

19 http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/
20 ibid.
21 ibid.
23 ibid.
to timely notify – in addition to negligence or breach of contract claims. There is no single federal notification rule so depending which state the corporation has interests, differing state regimes apply.

Corporate boards have a general duty to protect corporate assets, reputation, and goodwill. This typically includes overseeing systems to manage risk to the organization’s operations – including cyber risks. While the technical nature of cyber-based threats may be foreign to the typical corporate board, the same common sense, due-diligence approach that the board applies to other duties should be applied to cyber as well. The directors should have an understanding of the cyber risks which face the company and create an appropriate advisory team to determine what the “best practices” are to mitigate those risks. Boards should also engage in oversight of the programs in place, procedures, trainings, and any disclosures.

The general trend of US cyber regulations seem to point towards increased adoption of a “best practices” regime. While non-critical industries may not be directly regulated into following the NIST framework, the costs of not adopting such practices may outweigh the benefits – considering the potential legal penalties, regulatory fees, and loss of organization opportunities with more regulated industry.

**Forecasting the future U.S. cyber regulatory environment**

The general trend of U.S. cyber regulations seems to point towards increased adoption of a NIST-driven “best practices” regime. While non-critical industries may not be directly regulated into following the NIST framework, the costs of not adopting some clear cybersecurity practices may outweigh the benefits – considering the continuing growth in cyber-attacks against organizations in conjunction with potential legal penalties, regulatory fees, and loss of organization opportunities for those who lack “adequate” or “reasonable” protection schemes.

However, it should be noted that NIST is not the end-all-be-all of cyber resources. Standards from the SANS Institute, Open Web Application Security Project, and the Control Objectives for Information and Related Technology have also been referenced in recent regulatory expansions – offering readily available ancillary standards by which a company could use to design a legally “reasonable” cyber program.

**COUNSEL’S ADVICE AND “BOOM” PLANNING**

**Cyber-event as a “Boom”**

In the cybersecurity world, a cyber-event is typically referred to as a “boom”, with all pre-event planning actions taking place “left of boom” and all reactionary measures happening “right of boom.”

---

24 Ibid.
26 Ibid.
27 Ibid.
boom”. In the context of this “boom” centric framework, a typical CEO should seek to foster a multi-disciplinary team to deal with cyber concerns. In planning or in response to a cyberincident, coordinated action will be needed across multiple disciplines to help mitigate damage and recover functionality. A CEO will also seek close cooperation with legal counsel both “left of boom” and “right of boom.” Cybersecurity lawyers can help protect networks, systems, and data before they are compromised, as well as help mitigate the consequences of any cyber-incident which does occur.

TABLE 18.2 represents a RACI-style summary of the role of legal counsel and compliance both before and during/after a “boom”.

![enter Antonucci_Table_18.2_RASCI_role_Legal_20160821!]

**TABLE 18.2 RASCI matrix role for Legal Counsel and Compliance**

![end TABLE 18.2!]

**Left of Boom**

“The most important period of time in a company’s response to a cyber-incident likely occurs before the incident occurs.” Cyber breaches can happen quickly, not be detected for months, and then erupt into a volcano of trouble when discovered. Because of this volatility, the best way for a CEO to prepare the company for the legal requirements and ramifications of a breach is in substantial planning “left of boom.”

Without a specifically articulated regulatory standards for liability in a cyber-incident scenario, the CEO and Board should take steps to combat allegations of negligence or a violation of their fiduciary duty by showing that a “reasonable” degree of security has been put in place to guard against a cyber-incident. While the definition of what qualifies as a “reasonable” degree of security is still up for debate, a “process oriented” form of “reasonableness” is now widely adopted. To satisfy a “process oriented” standard, the CEO should develop a “process” to identify risks, delineate plans to deal with those risks, then implement the plans with requisite oversight. Actions taken towards fulfilling a “process” may have to be proven to regulators, shareholders, and judges in the event of a data incident – which makes the recordation of all c-suite and boardroom planning, discussion, and actions imminently important.

The basic “process” could be designed and executed by a board level advisory committee, comprised of multi-disciplinary professionals with some cyber familiarity. This *cyber committee* would be responsible for identifying cyber risk points and sensitive data, leading the creation and practicing of incident response plans, and ensuring that new security measures are

---

28 Cyber 5  
29 Cyber Playbook 5  
30 Cyber Playbook  
31 Handbook 49  
32 Handbook 48
constantly being incorporated into company’s cyber security apparatus – such as widespread data encryption practices depending on the data system. A system for reporting cyber-intrusions internally, with external partners in government or industry, and with regulatory or contractually required contacts should be developed and tested.

A board-level audit process should also be created to regularly review the advisory committee’s actions, plans, and recommendations. As previously mentioned, the audit’s methodology and findings should be written and preserved, as well as boardroom discussion over the audit’s results. In addition to audits, cyber-incident simulations can help identify holes in a potential cyber-response plan, as well as demonstrate dedication to a reasonable degree of “process” protection.

Legal should be deeply involved in the “left of boom” timeframe beyond articulating any applicable state or industry data regulations and directing documentation of the “process”. Past contracts should be revisited to ensure that included standards for the protection of proprietary information are being met, while future contracts should be written and examined with cybersecurity risks in mind.

Legal can help determine whether information sharing partnerships with government or with similar companies might be beneficial to a company’s cybersecurity prospects.

There should also be a discussion over the purchase of specific cyber insurance for organizations which manage considerable cyber risks.

“Boom” and right of “boom”

After a “boom” occurs and the organization is notified of the breach, a quick reaction holds the key to mitigating damage from the breach – and thus mitigating the potential expansion of liability from the breach.

The first response to a “boom” should come from the implementation of the prepared plan. Any response teams should be set in action with constant documentation of steps taken, with reports sent to the C-suite. A conversation with legal counsel — either with in-house or outside counsel depending on the potential need to preserve privilege — should be established immediately and sustained throughout the response to the crisis.

From the input of legal counsel, compliance with notification and data protection regulations pertaining to the subject industry should be adhered to. Beyond notification requirements, disclosure of the breach to partners in the private and public sector may create opportunities to gain further resources and information to mitigate damage. There may be some worry that disclosure to the government or public could harm the reputation of the company, this risk should be discussed and a strategy set. Owners of contractually transferred data should be notified as to the status of the breach and the confidentiality of their data. Notifying the public, and specifically those who might have had information disclosed by the breach, also warrants discussion with legal and other relevant parts of the company.

---

33 Playbook 5
As the response plan is implemented, an internal investigation should be created to record events and actions. If possible – observing the movements and tactics of the attackers within information systems can help inform how to scrub their access to the system, as well as providing known failure points to strengthen in future defensive measures.

While an "active defense," actively "hacking back" the hacking party, might seem attractive as a means to harry the offenders or to find out what data has been stolen – from a legal perspective it may do more harm than good. Using "active defense" beyond one's own networks can expose private organizations to expanded liability, including liability for "attacking" another network. If an "active defense" is necessary, receiving authorization from the foreign network owner before operations are commenced could help limit liability for actions taken.

CONCLUSION

The following cyber risk management statement represents those organization capabilities CEO and Board expect to be demonstrated in terms of cyber risk legal and compliance.

**Legal and Compliance.** The legal and compliance issues surrounding cybersecurity are pre-defined by principles of currency, reasonableness, and preparedness such that the organization is prepared for the legal requirements and ramifications of a breach. An organization must work with its legal professionals to ensure any currently applicable data security regulations are met while planning to accommodate regulatory expansion towards widely accepted standards. Legal should be integrally involved in the entire "process-oriented" cycle of cyber defense planning, including: committee creation, application, simulation, auditing, and recordation. The C-Suite must stay apprised on the process to ensure compliance with fiduciary duties and "reasonable" action (typically, to identify risks, delineate plans to deal with those risks, then implement the plans with requisite oversight). Actions towards fulfilling a "process" are able to be proven to regulators, shareholders, and judges in the event of a data incident via the recordation of all C-suite and boardroom planning, discussion, and actions. The basic "process" should be designed and executed by a board level advisory cyber committee, comprised of multi-disciplinary professionals with some cyber familiarity. A board-level audit process regularly reviews the advisory committee’s actions, plans, and recommendations. **Before any cyber event,** Legal Counsel not only articulates any applicable state or industry data regulations but directs documentation of the "process", reviews past contracts and manages future contracts with cybersecurity risks in mind. Legal can advise on the purchase of specific cyber insurances and determine whether information-sharing partnerships with government or with similar companies might be beneficial. **During and after** any incident, Legal Counsel is part of the response teams set in action with constant documentation of steps taken and with reports sent to the C-suite. Advice by legal counsel – either with in-house or outside counsel depending on the potential need to preserve privilege – should be established immediately and sustained throughout the response to the crisis. From the input of legal counsel, compliance with notification and data protection regulations pertaining to the subject industry is adhered to. Beyond notification requirements, disclosure of the breach to partners in the private and public sector may create opportunities to gain further resources and information to mitigate damage (whilst balancing internal concerns over potential harm the reputation of the company by such disclosure). **Owners**

---

34 See Playbook 7,
of contractually transferred data should be notified as to the status of the breach and the
certainty of their data. Notifying the public, and specifically those who might have had
information disclosed by the breach, also warrants discussion with legal and other relevant parts
of the company. An internal investigation should be created to record events and actions. If an
“active defense” is contemplated, receiving authorization from the appropriate public authorities
and foreign network owners before operations are commenced could help limit liability for
actions taken.

About the Cybersecurity Legal Task Force

The American Bar Association’s Cybersecurity Legal Task Force examines the risks posed by
criminals, terrorists, and nations that hope to steal personal and financial information, disrupt
critical infrastructure, and wage a new kind of warfare on a battlefield of ones and zeros. The
Task Force serves as a facilitator of collaboration, information exchange, and policy
identification in the emerging field of cybersecurity law

About Harvey Rishikof

Harvey Rishikof is co-chair of the American Bar Association National Cybersecurity Legal Task
Force. He formerly served as Chair of the American Bar Association Standing Committee on
Law and National Security and currently serves as its Advisory Committee Chair. He is Senior
Counsel at Crowell & Moring, LLP and is the former dean of the National War College in
Washington, D.C., where he also chaired the department of national security strategy. Mr.
Rishikof is a lifetime member of the American Law Institute and the Council on Foreign
Relations. Mr. Rishikof was a senior policy advisor to the Director of National
Counterintelligence, ODNI, a federal law clerk in the Third Circuit for the Honorable Leonard I.
Garth, a Social Studies Tutor at Harvard University, attorney at Hale and Dorr, A.A. to the Chief
Justice of the United States, legal counsel for the deputy director of the Federal Bureau of
Investigation, and dean of Roger Williams School of Law. Currently, he is also an advisor to the
Harvard Law Journal on National Security and serves on the Board of Visitors at the National
Intelligence University. He has written numerous articles, law reviews and book chapters. Mr.
Rishikof and Roger George recently co-authored The National Security Enterprise: Navigating
the Labyrinth (Georgetown Press, 2011); Patriots Debate with Steward Baker and Bernard
Horowitz (ABA Press, 2012); and A Playbook for Cyber Events; et.al. (ABA Press, 2014).

About Conor Sullivan

Conor is a joint Law and Masters of Public Administration candidate from Syracuse University’s
College of Law and Maxwell School of Citizenship slated to graduate in 2018. He is specializing
in national security law and is currently working as a Summer Law Clerk for the American Bar
Association’s Standing Committee on National Security. Conor has had work published by the
Syracuse University Honors Program, The End of the Means: Using the Arab Spring Revolutions
as a Case Study for Machiavelli’s The Prince, as well as by the National Defense University
Press, Responding to Russia after the NATO Summit: Unmanned Aerial Systems Overmatch in
the Black Sea.
Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics

Kelly Russo* and Harvey Rishikof**

INTRODUCTION

For all actors—government, business, and individual—cybersecurity has evolved significantly over the last fifteen years due to the rise of the Internet and the need for the free flow of information. Due to statutory divisions, we refer to cybersecurity as cybercrime, cyberespionage, and cyberwar. However, the evolution of security regulations can be examined through four periods beginning with pre-9/11 and progressing through the cyber era of today.

As the Internet expanded during the 1990s, it forced industry to focus on connecting systems and expand the flow of information, while the law, the Telecommunications Act of 1996, left the network largely unregulated. Some legislative attempts were made, but most failed. During this period, threats usually came from low-budget mischievous hackers, rather than criminals or nations. From the perspective of the U.S. government, terrorism and related security issues were almost exclusively issues dealt with overseas; it was an age of innocence.

After 9/11, a series of security-related laws and regulations were passed as attempts were made to lock down cyberspace. The Department of Homeland Security, Department of Justice, and Department of Defense began a nascent regulatory framework to strengthen security. The focus was “centered primarily on the

* Kelly Russo is an attorney with the Cybersecurity Legal Task Force at the American Bar Association in Washington D.C. She graduated from Wake Forest University, (B.A. 2012 cum) (J.D. 2015). While in law school, Ms. Russo served as the Marshal on the Moot Court Board, and was an Elite 8 Finalist at the Regional Jessup International Law Competition.

** Harvey Rishikof, American Bar Association Chair, Advisory Standing Committee on Law and National Security, is former legal counsel to the Deputy Director of the FBI, former Administrative Assistant to the Chief Justice of the United States, and former Dean of Roger Williams University School of Law. The opinions and views expressed in this Article are his own and do not reflect the opinions or views of any entity of the U.S. government.


2 Id.
16 ‘critical infrastructure’ sectors vital to the U.S., such as energy, chemicals, communications, financial services, and the defense industrial base.”

Almost exclusively, regulators focused on the security of physical spaces; however, some regulations were created to defend information systems from hackers disrupting critical operations. The legislation passed during this era included the USA Patriot Act of 2001, which permitted the use of more extensive investigative tools, harsher penalties, and intra-governmental information sharing. In 2001, the Department of Homeland Security (“DHS”) was created. In 2002, the Federal Information Security Management Act of 2002 established a cybersecurity framework for federal data systems. Then, in 2004, the Intelligence Reform and Terrorism Prevention Act of 2004, among other things, created the Director of National Intelligence.

In response to these developments, the ABA Cybersecurity Legal Task Force was created in 2012 under Former ABA President Laurel Bellows. It was established to examine ways to help lawyers protect their practices and their clients’ confidential information and intellectual property during cyber events, as well as position the ABA to contribute to national dialogue about cyber issues. It is tasked with addressing the tough questions about the appropriate role and responsibility of lawyers in cyber-related incidents and to examine ways that lawyers and businesses can protect their practices and their clients’ confidential information and intellectual property. It is composed of representatives of ABA entities having an interest in the cyber domain as well as leaders in the private and public sectors responsible for cybersecurity.

The Mission Statement for the Task Force was clear:

[To] identify and compile resources within the ABA that pertain to cybersecurity, and will focus and coordinate that ABA’s legal and policy analyses and assessments of proposals relating to cybersecurity… (1) Facilitate collaboration and information exchange among constituent ABA entities and with relevant public and private organizations; (2) Serve as a clearinghouse among ABA entities regarding cybersecurity activities, policy proposals, advocacy, publications and resources; (3) Study and analyze executive and legislative branch cybersecurity proposals; (4) Identify cyber-related issues for appropriate action by the ABA, including filling gaps in policy, encouraging ABA entities to develop new policy as appropriate, and sharing best practices

---

3 Id.
4 Id.
6 Id.
7 Id.
with members and their firms; and (5) Advise and assist ABA Governmental Affairs Office on cybersecurity advocacy and responses to government actions. 8

During the next period, regulations were focused more on protecting data, as data breaches affected a broad range of organizations, from corporations to the U.S. Office of Personnel Management. Regulators questioned the government’s role in ensuring cybersecurity and protecting private information. Information sharing between the public and private sector increasingly became the zone to ensure cybersecurity. Data theft in the last few years was perpetrated by criminals, spies, nations, terrorists, and “hactivists,” and “creating common, overarching standards for security, reporting, and response has proven to be a challenge . . . ” 9 This period was marked by tensions between the need for openness and creativity and the role of security and

---

8 About the Task Force, A.B.A., http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity/aboutcyber.html [http://perma.cc/87ZK-G7UC]. The Task Force was quite productive establishing principles, writing reports, and passing resolutions. Their Resolution of November of 2012 was comprised of the following five principles:

(1) Public-private frameworks are essential to successfully protect United States assets, infrastructure, and economic interests from cybersecurity attacks; (2) Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks; (3) Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements; (4) Privacy and civil liberties must remain a priority when developing cybersecurity law and policy; (5) Training, education, and workforce development of government and corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.

9 CROWELL & MORING, supra note 1, at 9.
safety. The Department of Defense implemented the Defense Federal Acquisition Regulation Supplement Safeguard Rule in 2013 requiring defense contractors to implement IT security controls. In 2014, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity was released, outlining the elements of a comprehensive cybersecurity program. Then, in 2015, President Obama issued an executive order that allowed the administration to impose sanctions on those that threaten U.S. infrastructure, and finally the Cybersecurity Information Sharing Act of 2015 was passed to improve information sharing between the government and private sector.

As we begin the year 2016, “data and information sharing will likely be woven more deeply into daily life.” Regulators will need to address the issue of privacy and the right to control information. Businesses and the government will be called on to implement security measures for a growing cyberworld. One of the most difficult challenges will be regulating global business as we attempt to navigate international efforts to ensure worldwide security. In this period, security measures will focus less on reacting to events and more on preventative measures. It will be all about finding the balance between privacy and security as we merge big data with small data. So how has the executive branch been navigating this balance thus far?

I. EXECUTIVE ORDERS REGARDING CYBERSECURITY

A. President Clinton

President Clinton signed the first executive order, Executive Order 13035, pertaining to the cyber sector on February 11, 1997. This order established the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet. The committee consisted of twenty-five or fewer non-Federal members appointed by the President. The purpose of this committee was to provide the National Science and Technology Council with guidance and information regarding “high-performance computing and

10 CROWELL & MORING, supra note 1.
11 Id.
13 CROWELL & MORING, supra note 1.
14 Small data refers to personal information belonging to an individual. Big data refers to information associated with corporations or government entities.
16 Id.
communications, Information Technology, and the Next Generation Internet."\textsuperscript{17} This included an independent assessment of progress in designing and implementing the Next Generation Internet Initiative and the High-Performance Computing and Communications Program. The order stated that the Department of Defense would provide the financial and administrative support to the committee.\textsuperscript{18}

Building on this framework, President Clinton also signed Executive Order 13133 on August 5, 1999, establishing the Working Group on Unlawful Conduct on the Internet, to report on the extent to which existing federal law offered an adequate basis for "effective investigation and prosecution of unlawful conduct that involves the use of the Internet."\textsuperscript{19} The Order also sought information and recommendations regarding new technological tools that might be necessary for effective investigation and prosecution of unlawful Internet use, as well as the availability of new or existing tools to educate the population and prevent unlawful conduct involving the Internet.\textsuperscript{20} The first attempts to organize the federal space met much resistance.

B. President Bush

President George W. Bush began with signing Executive Order 13231 on October 16, 2001, entitled "Critical Infrastructure Protection in the Information Age," with the purpose of encouraging "continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems."\textsuperscript{21} The order established the "President’s Critical Infrastructure Protection Board," to recommend policies and programs to "provide security and continuity to national security information systems."\textsuperscript{22} In doing so, the Board would consult and coordinate with the private sector, as well as state and local governments, to ensure that systems were established and maintained with the capacity to share threat warning, analysis, and recovery information. Again, there was much resistance from both inside and outside of government.\textsuperscript{23}

\textsuperscript{17} Id.
\textsuperscript{18} Id.
\textsuperscript{20} Id.
\textsuperscript{22} Id.
\textsuperscript{23} Id.
C. President Obama

Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, was signed by President Obama on October 7, 2011, in the wake of the WikiLeaks exposés. It encouraged reforms to improve the security of cyber networks that house sensitive information. It established multiple interagency groups to collaborate on security initiatives and put the burden of ensuring classified network security on "all agencies that operate or access classified computer networks." The Order also recognized the importance of information sharing and established the Senior Information Sharing and Safeguarding Steering Committee as well as the Classified Information Sharing and Safeguarding Office, to ensure safe sharing of information. Executive Order 13587 assigned the Secretary of Defense and the Director of the National Security Agency to serve as the Executive Agent for Safeguarding Classified Information on Computer Networks. It also created a government-wide Insider Threat Task Force to detect, deter, and mitigate cyberthreats.

President Obama's Executive Order 13636, entitled "Improving Critical Infrastructure Cybersecurity," was signed on February 12, 2013, to "improve cybersecurity information sharing and collaboratively develop and implement risk-based standards." The Order mandated the development of a "technology-neutral voluntary cybersecurity framework," in addition to promoting the adoption of cybersecurity practices and timely cyberthreat sharing. It also directed the incorporation of privacy and civil liberties protections and the exploration of using existing regulations and policies to promote cybersecurity. The Executive Order instructed the National Institute for Standards and Technology to collaborate with the private sector to establish best practices and create a cybersecurity framework. It also directed DHS to promote the implementation of the framework.

25 Id.
26 Id.
27 Id.
28 Id.
29 Id.
31 Id.
32 Id.
33 Id.
34 Id.
President Obama, seeing the need, signed Executive Order 13691, entitled “Promoting Private Sector Cybersecurity Information Sharing,” on February 13, 2015. The Order presented a framework for enhanced information sharing with the purpose of encouraging private sector companies to work together and work with the federal government to identify cyberthreats. The Order first “encourage[d] the voluntary formation of [organizations engaged in the sharing of information related to cybersecurity], to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organization to partner with the Federal Government on a voluntary basis.” The Order instructed DHS to create a non-profit organization to establish voluntary standards for the information sharing and analysis organizations (“ISAOs”) and authorized the Department to enter into information sharing agreements with ISAOs. Privacy concerns were also addressed, as the Order instructed private sector ISAOs to abide by voluntary standards of privacy protections when information sharing.

To grant the presidency more tools, President Obama signed Executive Order 13694, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” on April 1, 2015. This Executive Order regarded the recent cyberthreats as a national security emergency. It authorized the Secretary of the Treasury, in collaboration with the Attorney General and Secretary of State, to impose sanctions on those engaged in cyber-enabled activities that “are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States” and have the purpose or effect of “harming . . . entities in a critical infrastructure sector” with “significant disruption to the availability of a computer or network,” or “causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or

36 Id.
37 Id.
38 Id.
41 Id.
private financial gain.” The Executive Order also authorized the imposition of sanctions on those who knowingly receive or use trade secrets stolen by cyber-enabled activities (or provide material support) for financial gain when the theft threatens national security, foreign policy, or the financial stability of the country.\(^\text{43}\)

As one can see, the executive orders increasingly engaged the federal bureaucracy and searched for ways to engage the private sector.

II. CURRENT PENDING LEGISLATION

But one key to the puzzle remained: the need for legislation. Executive power alone would not be sufficient. The following bills on cybersecurity pending in the 114\(^\text{th}\) Congress were attempts to solve the issues. While several bills were proposed, those discussed below are the most comprehensive and the only then-pending cyber legislation with significant bipartisan support.

On Friday, December 18, 2015, lawmakers merged the first three information sharing cyber bills mentioned below into an omnibus spending plan, which was signed by President Obama. The Cybersecurity Act of 2015 includes an iteration of the Cybersecurity Information Sharing Act (“CISA”), which includes components from both the Protecting Cyber Networks Act (“PCNA”) and the National Cybersecurity Protection Advancement Act (“NCPAA”).\(^\text{44}\)

A. Protecting Cyber Networks Act, H.R. 1560

This bill was sponsored by Republican Devin Nunes from California and was introduced on March 24, 2015. It was passed 307-116 in the House on April 22, 2015 and was received in the Senate on April 27, 2015.\(^\text{45}\) The bill’s purpose was to encourage businesses to share information regarding cybersecurity risks by providing them protection from liability.\(^\text{46}\) Under the PCNA, the cyber information would be shared with civilian agencies, rather than DHS (as is the case with the NCPAA discussed below). The bill would require that businesses, prior to sharing information regarding a cybersecurity threat, “take reasonable efforts to

\(^{42}\) Id.
\(^{43}\) Id.
remove personal information identifying individuals related to the threat.”\textsuperscript{47} Additionally, the bill required the Privacy and Civil Liberties Oversight Board to address Congress and the President every two years with regard to the sufficiency of procedures to address privacy concerns.\textsuperscript{48}

The PCNA lists authorized uses of the information shared including: “cybersecurity, preventing death or serious bodily harm, preventing the exploitation of minors, preventing and prosecuting violent felonies, fraud and identity theft, and espionage and the theft of trade secrets.”\textsuperscript{49} Conversely, the NCPAA, discussed below, allows shared information to be used only for cybersecurity purposes.\textsuperscript{50}

While the NCPAA empowers DHS’s National Cybersecurity and Communications Integration Center (“NCCIC”) to serve as the main hub for public and private-sector information sharing, the PCNA does not designate a hub, but rather gives the President the power to establish a government hub or hubs with which the private sector can share information while explicitly prohibiting information sharing with the Department of Defense.\textsuperscript{51}

Critics of the bill argue that it does not include strong enough liability protections for non-federal entities.\textsuperscript{52} The PCNA states, “[n]o cause of action shall lie or be maintained in any court against any non-federal entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure if such sharing or receipt is conducted in good faith.”\textsuperscript{53} This “good faith” standard is regarded as a lower standard (than “willful misconduct,” for example) of proof and opens businesses up to a greater risk of litigation.\textsuperscript{54}

Critics also attacked the bill’s privacy protections, arguing that the bill would give companies the ability to share data with intelligence agencies, allowing them to ignore laws like the Privacy Act of 1974 and the Electronic Communication Privacy

\textsuperscript{48} Id. § 107.
\textsuperscript{50} Id.
\textsuperscript{51} David Eppstein, Cyber Bills Compared (Dec. 17, 2015) (unpublished working paper) (on file with author); see also H.R. 1560 § 103.
\textsuperscript{52} Inserra & Walters, supra note 49.
\textsuperscript{53} H.R. 1560 § 106(b).
\textsuperscript{54} Id.
Act of 1986. However, proponents of the bill argued that there are strong privacy protections because the bill limits the categories of sharable information to only the listed cyber threat indicators and requires two scrub of personal information from the shared information: one by the private sector business and one by the government.

B. National Cybersecurity Protection Advancement Act, H.R. 1731

This bill was sponsored by Republican Michael McCaul from Texas and was introduced on April 13, 2015. The House Homeland Security Committee passed it nearly unanimously. It was designed to provide liability protections to those businesses who voluntarily share data regarding cyber threat indicators and defensive measures with one another and with DHS’s NCCIC. The bill would grant liability for private businesses to perform network awareness sweeps of their own data systems and would permit the NCCIC to share information concerning cybersecurity threats with private businesses, in addition to other non-federal bodies. Without these liability protections, businesses sharing information pursuant to this bill could expose themselves to class actions or regulatory enforcement actions.

The NCPA included several provisions limiting the privacy threat of information sharing, such as a prohibition on federal use of shared data to engage in surveillance for the purpose of tracking persons’ individually identifiable information. The bill also required DHS to create and review annually privacy policies and processes that direct the “receipt, retention, use, and disclosure” of information shared with NCCIC in accordance with the bill. Another privacy protection in the NCPA would require private businesses to remove all personal information that is not related to the cyber threat before sharing the information with the NCCIC or private bodies. The NCCIC

58. Id.
61. H.R. 1731 § 3.
62. Id.
63. Id.
would then be required to conduct a second screening in order to ensure that there is no personal information unrelated to the cyberthreat before sharing the information with other government or private groups.\textsuperscript{64}

This bill was viewed by technology, telecommunications, and infrastructure businesses as "a critical compliment to the PCNA."\textsuperscript{65} It also was viewed as favorably expansive, allowing the NCCIC to include tribal governments, information sharing and analysis groups, and the private sector, in addition to expanding the NCCIC's functions to include global cybersecurity measures with international partners.\textsuperscript{66} Its liability protection had been given positive reviews as well. The NCPAA states that a "non-federal entity . . . shall not be liable in any civil or criminal action brought under this subsection unless such non-federal entity engaged in willful misconduct or gross negligence with respect to sharing or conduct and such gross negligence or willful misconduct proximately caused the injury."\textsuperscript{67} The standard of "willful misconduct or gross negligence" is a strong standard and protects businesses, and thus incentivizes the sharing of cyber information.\textsuperscript{68}

While the liability provisions of the NCPAA were strong and widely praised, critics suggested that the bill could be improved by broadening the authorized uses of the shared information, as the NCPAA restricts the government use to just "cybersecurity purposes."\textsuperscript{69} Critics suggested allowing the government's use of properly shared information as long as one significant use is for cybersecurity purposes, pointing to the authorized uses in the PCNA as a model.\textsuperscript{70}

C. Cybersecurity Information Sharing Act of 2015, S. 754

Republican Senator Richard Burr from North Carolina sponsored this bill. It is the Senate counterpart to the PCNA and was introduced on March 17, 2015, and passed 74-21 in the Senate on October 27, 2015.\textsuperscript{71} CISA would provide liability protections to companies of the private sector that share information about security breaches or vulnerabilities with

\textsuperscript{64}\textit{Id.}
\textsuperscript{65} Farris & Kessler, \textit{supra} note 60.
\textsuperscript{66}\textit{Id.}
\textsuperscript{67} H.R. 1731.
\textsuperscript{68} Insera & Walters, \textit{supra} note 50.
\textsuperscript{69}\textit{Id.}
\textsuperscript{70}\textit{Id.}
particular government entities. Like the PCNA, CISA would authorize voluntary sharing of information between the government and private companies through a portal established by DHS.\textsuperscript{72} Also similar to PCNA, CISA would protect information shared against disclosure under the Freedom of Information Act and similar state laws.\textsuperscript{73} Both the PCNA and the CISA would also provide protection from private suits and would codify Federal Trade Commission and Department of Justice policy that cybersecurity information sharing does not encroach upon antitrust laws.\textsuperscript{74}

Critics of the CISA, including major technology companies, like Apple, Twitter, and Reddit, argued that the bill has major privacy and Internet security concerns. First, they argue that CISA would allow surveillance of Internet users and does not include adequate privacy protections of personal information. Second, it does not include any recourse for consumers if their personal information were to be improperly shared with the federal government. Third, the liability protections in the bill would discourage businesses from improving their own security measures.\textsuperscript{75}

All three of these information sharing bills contain a federal preemption clause, meaning they would supersede any state statutes or provisions of state law that regulate an activity expressly authorized under one of these bills. This could limit states’ ability to combat cyberthreats, which are sometimes arguably better equipped to collaborate with the private sector to prevent cyberthreats.

D. Cybersecurity Act of 2015

The Cybersecurity Act of 2015, which is Division N of the most recent omnibus spending bill, was passed by Congress and signed by President Obama on December 18, 2015.\textsuperscript{76} The Act establishes a voluntary cybersecurity information sharing procedure that encourages public and private entities to share


\textsuperscript{75} See Summaries for the Cybersecurity Information Sharing Act of 2015, \textit{supra} note 72.

cyberthreat information with one another. Despite the outpour of divided reactions from various supporters and critics, the Act is meant to serve as a piece of compromise legislation, as provisions of both the PCNA and NCPAA influence it. However, it does not include language from the two pieces of pending legislation discussed below.

Under the Act, the federal government is instructed to establish procedures for sharing classified and unclassified cyberthreat indicators and defensive measures with the private sector. The Act’s key information sharing provision states, “[a] non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.” The private sector may only share data that falls within the Act’s definitions of “cyber threat indicator” or “defensive measure.” The Act defines a cyberthreat indicator as “information that is necessary to describe or identify [a cyberthreat].” A defensive measure is “an action, device, procedure, signature, technique, or other measure” that “detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.” Additionally, before sharing any information, the private sector entity must remove information that it “knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

The Act tasks DHS with the job of creating a mechanism by which the government can receive cyberthreat indicators and defensive measures from the private sector. In real time, DHS must then share the information with the appropriate federal entities, including the Office of the Director of National Intelligence and the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury. It also allows the President to designate other federal entities (in addition to DHS) to develop an information sharing process, excluding the Department of Defense.

---

77 Id.
80 Id. § 104(c)(1), 129 Stat. at 2942.
81 Id. § 102(d), 129 Stat. at 2938.
82 Id. § 102(7), 129 Stat. at 2938.
83 Id. § 104(d)(2)(A), 129 Stat. at 2943.
84 Id. § 102(3), 129 Stat. at 2937; see also id. § 105(a)(3)(A), 129 Stat. at 2945.
85 Id. § 105(c)(2)(B), 129 Stat. at 2948.
The Act provides several privacy protections for those entities that choose to participate in information sharing. First, it limits the government’s use of the shared information to use only for a “cybersecurity purpose,” meaning “the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.” 86 Second, the Act prevents federal agencies from disseminating the shared information, which the Act exempts from disclosure under the Freedom of Information Act. 87 Third, the private sector is immune from liability for sharing or receiving cyberthreat indicators or defensive measures. 88

There have been varying degrees of support and opposition in response to the passing of the Cybersecurity Act. Supporters of information sharing believe that the increase in information sharing will improve the overall cybersecurity of our country. They argue that the Act has ample privacy protections and is voluntary. Critics call the Act a “surveillance bill” that encroaches upon privacy rights, and Section 104 of the Act, the key provision relating to Internet surveillance, has become a popular topic of discussion. 89 Section 104 allows network operators to take three steps only “for cybersecurity purposes.” Network operators can (1) monitor, (2) operate defensive measures, and (3) share information. Additionally, with written consent, a network operator can allow an outside entity to monitor its network and operate defensive measures. 90 Those that oppose Section 104 argue that it gives a network operator too much power with little to no guidance or limitations. For example, the Act allows monitoring for “cybersecurity purposes,” which is arguably broad and unclear. 91

E. Bills Not Incorporated into the Act of 2015

1. Data Security and Breach Notification Act of 2015

Not incorporated into the Cybersecurity Information Sharing Act of 2015 were two pieces of pending legislation dealing with

86 Id. § 103(4), 129 Stat. at 2937.
87 Id. § 103(d)(3), 129 Stat. at 2950.
88 Id. § 106(a)–(b), 129 Stat. at 2951–52.
90 Id. § 104, 129 Stat. at 2940–43.
state power and resources. On December 9, 2015, the House Financial Services Committee approved the Data Security Act of 2015 by a 46-9 vote. This act would supplant 47 state laws with a single national statute, requiring minimum-security protections at businesses in the private sector and establishing a national requirement for data breach notification. The private sector is generally in favor of a single law because it will provide a uniform standard to comply with, as opposed to various state laws. The legislation "identifies security controls organizations should adopt, including those involving access controls and restrictions, use of encryption of sensitive information and monitoring systems. The bill also directs businesses to require their third-party service providers to implement appropriate safeguards for sensitive information."\textsuperscript{92}

The Data Security Act would allow businesses in different sectors to adopt security procedures that would work best with their specific needs. Regulatory enforcement would occur among several different agencies, including the Federal Trade Commission, the Comptroller of the Currency, the Federal Reserve System, and the Securities and Exchange Commission, among others. Business entities covered by the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act would be exempt from the Data Security Act.\textsuperscript{93}

Critics of the legislation, including Democratic Representative Denny Heck from Washington, believe it takes the power to regulate security among insurers away from states' insurance commissioners, whom Heck contends work smoothly together. The legislation would also usurp laws in twelve states that call for businesses in their jurisdiction to adopt particular IT security procedures.\textsuperscript{94} Massachusetts Assistant Attorney General Sara Cable testified before Congress earlier this year and contended that preempting state laws "represents a significant retraction of existing protections for consumers at a time when such protections are imperative. Minimum data security standards are important and necessary, but the proposed standards leave consumers' data vulnerable."\textsuperscript{95} This led Democrat Maxine Waters of California to present an amendment that would allow states to provide more stringent security requirements. However, the


\textsuperscript{93} Id.

\textsuperscript{94} Id.

\textsuperscript{95} Id.
panel struck down the amendment on a voice vote, as Massachusetts was the only state that had stronger data security requirements than those presented in the Data Security Act.\textsuperscript{96}

Critics also believe that this one-size-fits-all approach to cybersecurity will not be effective. Jennifer Safavian, an executive vice president at the Retail Industry Leaders Association, stated in a letter sent to the Committee’s leaders that “[h]aphazardly slapping rules that were written 15 years ago for the financial industry on retailers, restaurants and thousands of small businesses is not the kind of data security legislation that will safeguard our economy.”\textsuperscript{97}

Privacy advocates, as well as consumer protection organizations, argue that the legislation would weaken consumer protections by stifling new and/or developing state laws that extend data security and breach notification protections to online account login systems. They argue that the bill would also abolish all opportunities of redress for consumers.\textsuperscript{98} In a December 7, 2015 letter to the Committee’s leaders, seventeen privacy and protection groups wrote: “If this bill were to pass, state attorneys general would be limited to seeking civil penalties and injunctive relief, even in cases where consumers suffer extensive harm as a result of a breach of highly sensitive information.”\textsuperscript{99}

2. State and Local Cyber Protection Act of 2015, H.R. 3869

On December 10, 2015, the House unanimously passed a bill that would provide state and local government with federal funds to battle cybercrime.\textsuperscript{100} The bill’s sponsor is Republican Representative Will Hurd from Texas. He is a former CIA officer who focused on cybersecurity and now chairs the House Oversight Subcommittee on Information Technology. Hurd stated, “[l]ocal governments often do not have access to the technical capabilities and training required to address highly exploitable cybersecurity vulnerabilities.”\textsuperscript{101} The bill amends the Homeland Security Act of 2002 to require the National

\textsuperscript{96} Id.
\textsuperscript{97} Id. (quoting Jennifer Safavian).
\textsuperscript{98} Id.
\textsuperscript{99} Id. (quoting letter from privacy and consumer protection groups).
\textsuperscript{100} H.R. 3869 – State and Local Cyber Protection Act of 2015, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/3869/actions?q=%7B%22search%22%7D\%3A%5B%22hr3869%22%5D\%3A%5D&resultIndex=1 [http://perma.cc/FLG-EYUH].
Cybersecurity and Communications Integration Center ("NCCIC"), DHS’s cyber group, to assist state and local governments with technical and strategic training to enhance their cyber defense.\footnote{State and Local Cyber Protection Act of 2015, H.R. 3869, 114th Cong. § 2.} The NCCIC is tasked with aiding state and local governments with identifying vulnerabilities in their systems, providing guidelines and information related to information security, conducting trainings on cybersecurity, and providing technical assistance with regard to implementing security systems.\footnote{Id.} The bill is now awaiting further action in the Senate.\footnote{Williams, supra note 101.}

III. CYBERATTACK HOT TOPICS LEFT OPEN

Although the Cybersecurity Act of 2015 is a sound first step, there are a number of issues that still need to be resolved. With the evolution of technology, ensuring sound cyber protections and preventing attacks has become increasingly important and increasingly difficult. Even the federal government is having difficulties enlisting the tech industry to help fight terrorism. While the tech community is willing to help, it is reluctant to reveal private information and data to the government for fear of user distrust and the misuse of sensitive information. White House representatives traveled to Silicon Valley in early January 2016 in an effort to convince tech companies of the importance of working with the government to keep our country safe. Needless to say, there was push back. A chief security officer at the tech company Twistlock pleaded with the “Obama administration to consider alternative forms of intelligence gathering now that encryption technology has become so common.”\footnote{W.J. Hennigan & Parsh Dave Tracey Lien, White House Presses Silicon Valley to Aid in Terrorism Fight, SEATTLE TIMES (Jan. 9, 2016, 3:49 PM), http://www.seattletimes.com/nation-world/white-house-presses-silicon-valley-to-aid-in-terrorism-fight/ [http://perma.cc/L24N-U4C3].} There is a “Washington” v. “Silicon Valley” divide concerning how best to deal with cybersecurity.

Nevertheless, the tech community is willing to work with the government as long as proper protections are in place. After the meeting, Facebook noted that tech companies and the government were “united in [their] goal to keep terrorists and terror-promoting material off the Internet.”\footnote{Id.} This strained safety/privacy conversation between White House representatives and Silicon Valley tech experts serves as an example of the many complications involved in cybersecurity. While terrorism is one worry associated with the ever-evolving
cyberworld, the following issues of privacy, encryption, liability, and cyber insurance are at the forefront of concerns and debates.

A. Privacy—Who Owns the Information?

While there are many benefits to increasing data, connectivity, and other cyberservices, the developments in the cyberworld pose difficult challenges to ensuring privacy of sensitive information. Julie Brill of the U.S. Federal Trade Commission ("FTC") is one of the leaders in analyzing privacy and data security issues. In her recent speech at the Washington Governor Jay Inslee’s Cyber Security and Privacy Summit, Brill stressed, "[c]onsumers want to know – and should be able easily to find out – what information companies are collecting, where they're sending it, and how they're using it. This kind of information is important to consumers' decisions about whether to use digital products and services in the first place."107 She also mentioned the work the FTC has done to protect the privacy interests of consumers. For example, the FTC has brought actions against companies for inappropriately collecting private information from mobile devices and for revealing confidential health and other sensitive information.108 In addition to the work of the FTC, other federal regulators, as well as state governments have enhanced privacy protections for consumers, but there is much more work to be done.109

One of the most widely discussed privacy issues with regard to cybersecurity centers around cyber information sharing between private entities and the government. Privacy and civil liberties groups cite many issues surrounding companies' duty to remove personally identifiable information ("PII") before sharing with the government. Critics are also skeptical about what the government does with this information when it is received and whether or not it is safely stored.110 This debate is at the heart of the intersection of small and big data.

Privacy and civil liberties groups claim privacy concerns as the reason for their opposition towards the new cybersecurity bill signed by President Obama on December 18, 2015. They argue that the definition of acceptable information to share is too broad

108 Id. at 3.
109 Id. at 4.
and the burden placed on companies to erase PII is not strict enough.¹¹¹ Nonetheless, the final version of the cybersecurity bill "compels entities to remove information they 'know' is extraneous personal information."¹¹² This is a higher standard than previous versions of the bill that used "reasonably believe" instead.¹¹³

Furthermore, DHS is sponsoring the nonprofit group Mitre Corporation's development of the Structured Threat Information eXpression ("STIX"). This would provide a "common language and mechanism for quickly analyzing, sharing, and receiving cyber threat information."¹¹⁴ The adoption of a common sharing scheme would improve privacy, as there would be clearer guidelines as to what vulnerable information is shared and what is not.

Privacy issues also arise in the context of data breach reporting after a cyberattack has occurred. While there is no federal data breach statute, almost all of the states have data breach notification laws. Most state breach notification statutes are similar, however some do vary in several ways including: what constitutes a breach, what data is considered PII, and when a notification should be filed.¹¹⁵ Most states agree on the general definition of PII—the attachment of certain information connected to someone's first and last name. However, states have not uniformly agreed upon what constitutes PII. For example, some states do not consider medical information, health insurance information, and email addresses to be PII.¹¹⁶

As the Internet and data sharing defy borders, privacy concerns do not affect the U.S. in isolation. The European Union’s new data privacy law and the newly passed U.S. Cybersecurity Act set the tone for a pending U.S.-EU data sharing agreement to replace the Safe Harbor, which expedited the transfer of data between businesses and international networks. The EU’s new data privacy regulations have been deemed more burdensome for U.S. companies and aim to protect the consumer. This could affect U.S. companies operating in the

¹¹² Id.
¹¹³ Id.
¹¹⁵ JUDITH MILLER ET AL., A PLAYBOOK FOR CYBER EVENTS 39 (2d ed. 2014).
¹¹⁶ Id. at 39–40.
EU if they are held to the new standards. In the coming months, we will see how the EU-U.S. negotiations play out and how that will affect international privacy concerns.\footnote{Stephen Dockery, \textit{EU Data Law Shows Way Forward for Next Safe Harbor Agreement}, \textit{Wall St. J.} (Dec. 18, 2015, 3:25 PM), http://blogs.wsj.com/riskandcompliance/2015/12/18/eu-data-law-shows-way-forward-for-next-safe-harbor-agreement/.}

B. Encryption—How Is Access to Be Granted to Information?

Encrypting data alters readable information into unreadable information except to authorized readers. This prevents anyone who steals data from reading it, rendering the stolen data worthless to cybercriminals. In addition to protecting data, companies encrypt data because it may exempt a company from particular regulatory requirements, such as some state data breach notification statutes. Some downsides to encryption include the time and effort it takes to encrypt all data, the cost, and the potential for slowed operating performance. While encryption/decryption occurs automatically for authorized readers, the process can require significant computing power and memory that can slow computer systems and affect productivity within the company. Therefore, it is most common for companies to encrypt some, but not all data.\footnote{Id. at 14.}

It is important to note that encryption does not fully protect a company, as encryption only protects data and not the security of networks and systems. Furthermore, companies must securely store and protect decryption keys/algorithms that could get in the hands of cybercriminals.\footnote{Joe Uchill, \textit{Both Sides of Data Encryption Debate Face Off in Congress}, \textit{Christian Science Monitor} (Apr. 30, 2015), http://www.csmonitor.com/World/Passescode/2015/0430/Both-sides-of-data-encryption-debate-face-off-in-Congress [http://perma.cc/YJ6P-M24J].}

Lawmakers have considered the argument in favor of strong encryption requirements as a means of protecting data from cyberattacks, as well as the argument against encryption by those who argue that it could hamper law enforcement efforts, as communication via encryption could allow terrorist and other criminals to avoid surveillance. The problem with providing law enforcement "back door" access is that cybercriminals could easily misuse it, or sophisticated cybercriminals could communicate via unsanctioned encrypted data that does not contain a back door, and thus, would prevent law enforcement from accessing the data.

In his article, "Be Careful What You Wish For: Device Hacking and the Law," cybersecurity expert Benjamin Witte
2016] Cybersecurity

theoretically discusses the legal implications of allowing the government to bypass encryption systems, as opposed to requiring decryption. This would occur through the "exploitation of existing vulnerabilities to accomplish legally authorized wiretapping."\(^{121}\) Wittes warns that allowing the government to bypass encryption systems would deprive the private sector of key legal protections. The scope of the information hacked would have no limit. It would also be unclear as to whether the carrier would be required to assist the government in installing the malware. He believes that in the context of a lawsuit, courts would ask whether the government's request for technical assistance is "unduly burdensome for companies," which has not been clearly defined. All in all, Wittes believes that lawful hacking would lead to the "government's commandeering companies into compromising their users' devices."\(^{122}\)

This debate has its roots in the Communications Assistance to Law Enforcement Act of 1994, when telephone companies were required to assent to lawful wiretaps. As noted by the recent Harvard Berkman Center report, *Don't Panic: Making Progress on the "Going Dark" Debate*, the world of the Internet of Things has changed the playing field for encryption, and that is not that easy to achieve as world wide web standards and key elements of communication such as metadata and weak software provide many avenues for the state. As before, there is much debate over the ground truth concerning technical issues and the implications for the market and policy.\(^{123}\)

Apple is now litigating the scope of the technical assistance language in the Wiretap Act, which requires carriers to assist government agents in lawful wiretaps. One potential public policy impact of requiring Apple to push government malware is that it could lead to a serious lack of trust in Apple and other service providers. Wittes believes that the case will likely turn on how difficult it would be for a company like Apple to unobtrusively send malware to its users. He mentions that it may also turn on who writes the malware.\(^{124}\)

Despite the lawsuits, media attention, and airtime the topic of encryption has received at both the Republican and


\(^{122}\) Id.

\(^{123}\) Matt Olsen et al., *Forward to Berkman Center, Don't Panic: Making Progress on the "Going Dark" Debate* (2016).

\(^{124}\) Wittes, *supra* note 121.
Democratic presidential debates, at this point there is no strong legislative push to give law enforcement access to encrypted data.\textsuperscript{125}

C. Liability—Who Will Pay for Information Violations?

One of the most prevalent topics with regard to liability is information-sharing relevant to liability protections. In order to encourage businesses to share cyberthreat information with the government and other private sector companies, there must be liability protections to shield companies from lawsuits surrounding the shared data. The U.S. Department of Justice and the Federal Trade Commission jointly issued a Policy Statement in April 2014 acknowledging that antitrust laws do not attach liability to cybersecurity information sharing “as long as the sharing does not encroach on competitively sensitive information related to price, cost or output.”\textsuperscript{126} The agencies reasoned that the type of information shared in cyber information sharing is typically “very technical in nature and very different from the sharing of competitively sensitive information.”\textsuperscript{127} The White House agreed and President Obama stressed the importance of information sharing in Executive Order 13636.\textsuperscript{128} Currently, companies are shielded from liability when sharing “cyber threat indicators,” arguably a narrow liability protection.

Liability concerns for breached companies also involve private suits. It varies from state to state whether private actions can be brought against breached companies. Some do not allow any private suits, while others allow suits to recover damages. Suits are brought by clients, customers, vendors, and other business associates of the breached company. Courts are split on whether the data must be misused before a plaintiff can sue.\textsuperscript{129} The new legislation affords some indemnification if the information is shared with DHS, but it is unclear what potential liability awaits from other regulatory agencies such as the FTC or the SEC.\textsuperscript{130}

D. Cyber Insurance—How Will Risk over Information Be Allocated?

There are many expenses that a company may incur from a cyberattack. The expenses may involve: notification of clients, government agencies, credit monitoring services, forensic costs

\textsuperscript{126} Navetta & Mathur, supra note Error! Bookmark not defined..
\textsuperscript{127} Id.
\textsuperscript{128} Id.
\textsuperscript{129} Miller et al., supra note 115, at 40.
involved in the investigation, and legal costs surrounding claims or suits, as well as business interruption or the payment of judgments or settlements. The average cost of a cyberattack was $7.2 million in March 2011 and has likely risen since then. The majority of cost comes from the time and resources expended surrounding notification requirements.\textsuperscript{131}

While resilient security systems may prevent most cyberattacks, there are some cyber intrusions that cannot be prevented, such as a zero-day attack.\textsuperscript{132} In order to protect one’s company from incurring the exorbitant costs that follow unpreventable breaches, cyber insurance has become more and more common. There are several types of insurance with varying degrees of protection. It is important to understand all the exclusions and gaps in coverage. Oftentimes multiple plans are necessary in order to have adequate protection. Insurance services organization commercial property policies may cover losses as a result of a virus, but oftentimes the policy requires the data to have been destroyed or corrupted.\textsuperscript{133} General liability insurance covers only physical injury, in addition to liability as a result of publication of private material.\textsuperscript{134} Professional liability insurance is limited by the term “professional services” or by exclusions.\textsuperscript{135} Policies like the surety and fidelity computer crime policy oftentimes do not cover losses resulting from theft of private information, indirect consequential loss, and potential income.\textsuperscript{136}

Cyber liability insurance is often offered as a stand-alone insurance policy with combined third-party liability and first-party coverage. It is designed to cover insureds that transmit and store private consumer data.\textsuperscript{137} It is extremely important to review the coverage one’s company has in place before an attack occurs in order to ensure adequate coverage. At this time, cyber liability insurance coverage can include: data breach/privacy crisis management (i.e. investigation, data notification, legal costs etc.), media liability (i.e. defamation of website and intellectual property rights infringement), extortion liability (i.e. losses due to threat of extortion), and network security (i.e. damages due to denial of access, costs related to theft of third-party data).\textsuperscript{138} One advantage from a system

\textsuperscript{131} RHODES & POLLEY, supra note 5, at 192–93.
\textsuperscript{133} See RHODES & POLLEY, supra note 5, at 192–93.
\textsuperscript{134} Id. at 193.
\textsuperscript{135} Id.
\textsuperscript{136} Id. at 192–93.
\textsuperscript{137} Id. at 194.
\textsuperscript{138} Sarb Sembhi, An Introduction to Cyber Liability Insurance Cover, CONSUMER
perspective is that as insurance coverage expands, more elements of the private sector will enhance coverage to meet policy requirements.

CONCLUSION—THE CURRENT BATTLE SPACE

Cybersecurity is hard because it requires the forging of the "geek-wonk" bridge. It involves the blending of technical and policy cultures. Moreover, to engage society in this arena, we have four large social hammers—legislation, insurance premiums, tax policy, and lawsuits. Increasingly we are seeing movement in each of these policy areas. In short, both carrots and sticks are being deployed against corporate America.

But our adversaries are not resting. The recently released report from the Defense Security Service provides a snapshot into the current state of the world’s cybersecurity situation, detailing specific regions and industries at risk.\(^\text{139}\) The report states that in the last year there has been an eight percent increase in reported foreign collection attempts to obtain sensitive or classified data in the U.S. cleared industrial base.\(^\text{140}\) East Asia and the Pacific was the top collector region and the threat level from this region was labeled "critical."\(^\text{141}\) The electronics sector topped the list as the most targeted sector, while the commercial sector remained the top collector affiliation.\(^\text{142}\) Academic solicitation was reported as the top method of operation.\(^\text{143}\) In order to prevent these threats and enhance national and global cybersecurity, the government and the private sector must balance security and privacy interests through a concise set of agreed-upon standards and approaches necessary to build worldwide cybersecurity. Waiting is no longer an option.


\(^{\text{140}}\) Id.

\(^{\text{141}}\) Id.

\(^{\text{142}}\) Id.

\(^{\text{143}}\) Id. at 12.
In the last few days, Secretary of Homeland Security Jeh Johnson and Homeland Security Advisor Lisa Monaco have both suggested that in the wake of the DNC hack, the United States is considering designating its election system as critical infrastructure. That's a good idea. Designating election infrastructure as “critical” captures the commonsense notion that protecting elections from cyber-enabled manipulation is very important. The designation also has implications for preparing for and responding to cybersecurity incidents, including pursuant to Presidential Policy Directive-21 and last week’s Presidential Policy Directive-41.

But designating election-related systems as critical infrastructure would also provide an opportunity to socialize a norm against cyber-enabled interference with elections at the international level. As debates continue about how the United States should respond to the alleged Russian hack of the DNC, a new U.N. Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security will convene this month in New York. The United States can use the GGE process to set down a clear marker that election infrastructure is part of the critical infrastructure that last year’s GGE agreed should not be attacked in peacetime.

The DNC hack and subsequent information dumps on WikiLeaks have brought cybersecurity concerns about elections into the public debate, but experts have highlighted security problems with voting machines—particularly ones that don’t produce paper audit trails—for more than a decade. (For an overview of that history, see here.) Bruce Schneier argued in the Washington Post last week that before November “we must . . . create tiger teams to test the machines’ and systems’ resistance to attack, drastically increase their cyber-defenses and take them offline if we can’t guarantee their security online.”

Along with upping its defenses, the United States should take the opportunity provided by the new GGE process to push for agreement on a norm against interference with election infrastructure. Last year’s GGE report accepted a U.S.-proposed norm against attacking critical infrastructure in peacetime, but left undefined what constitutes critical infrastructure. Specifically, the GGE member states (including Russia) agreed that, “A State should not conduct or knowingly support [information and communications technology or] ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public,” (para. 13(f)), and that “States should . . . respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty” (para. 13(h)). The GGE report did not define “critical infrastructure,” but called for “[t]he voluntary provision by States of their national views of categories of infrastructure that they consider critical” (para. 16(d)).

The United States should clarify in this year’s GGE that election infrastructure counts as critical infrastructure in the United States. I pointed out last summer that:

[a]s a domestic matter, the United States has defined critical infrastructure very broadly to include 16 sectors, such as communications, the defense industrial base, financial services, nuclear reactors, and transportation. But some of the sectors are less obvious. The Department of Homeland Security lists as examples of the “commercial facilities sector” professional sports leagues, casinos, campgrounds, and motion picture studios. Many countries might be surprised to discover that the United States considers the Iranian hack of the Las Vegas Sands Corporation and the North Korean hack of Sony Pictures to be attacks on “critical infrastructure.” To avoid creating potentially dangerous confusion over what the norm encompasses, the GGE should agree . . . to a definition of critical infrastructure in the international sphere.
Expanding the U.S. definition of critical infrastructure to include election infrastructure in time to make a stand with GGE members could help to promote an international norm against cyber-enabled meddling in elections. It could also send a clear signal about the seriousness with which the United States would regard intrusions aimed at interfering with the integrity of this fall’s elections.

GGE agreement would not, of course, be a panacea. Compliance in practice is different from agreement in principle. And it’s not perfectly clear what would count as election infrastructure in the United States or abroad. Nonetheless, while the U.S. government considers possible responses to Russia over the DNC hack, the GGE process provides a chance to build a coalition against cyber-enabled election interference.

Tags: 2016 Presidential Elections, Critical Infrastructure, Cyber, Cyber Warfare, Cybersecurity, DHS, DNC Hack, International Law, Russia, United Nations

ABOUT THE AUTHOR

Kristen Eichensehr is an Assistant Professor at UCLA School of Law. She previously served as Special Assistant to the Legal Adviser of the U.S. Department of State. Follow her on Twitter (@K_Eichensehr).

SEND A LETTER TO THE EDITOR
Risky Business: When Governments Do Not Attribute State-Sponsored Cyberattacks

by Guest Blogger
October 4, 2016

Kristen Eichensehr is an Assistant Professor at UCLA School of Law, an affiliate scholar at the Center for Internet and Society at Stanford Law School, and a term member of the Council on Foreign Relations.

In the presidential debate last week, Hillary Clinton cited Russia’s responsibility for the hack of the Democratic National Committee (DNC). Two weeks ago, Senator Diane Feinstein and Congressman Adam Schiff released a statement explaining, “Based on briefings we have received, we have concluded that the Russian intelligence agencies are making a serious and concerted effort to influence the U.S. election.” Despite these statements and Crowdstrike’s accusations against Russia, the executive branch has not officially attributed the DNC intrusions to Russia.

In the absence of official attribution by the U.S. executive branch, private cybersecurity companies are playing the role of accusers of foreign governments. The DNC compromise is not the only case like this. Take the 2015 Office of Personnel Management breach. The executive branch has not formally identified the perpetrators of that intrusion either, but Crowdstrike has accused Chinese government-affiliated hackers.
Casting private companies in the role of accusers has some benefits, but relying on private attributions to the exclusion of official attributions may create some underappreciated risks for the United States.

On the plus side, attributions by private companies have fostered transparency: the companies publicly announce their findings and release reports—often quite detailed ones—about their evidence. Other companies and researchers can then independently evaluate the evidence and confirm or dispute the attribution. That double-checking process confirmed Crowdstrike’s attribution of the DNC hack to Russia. Attribution by companies can also put foreign government-sponsored hackers on notice that their actions are traceable, potentially deterring or at least slowing further intrusions.

U.S. government officials have praised private attributions and suggested they are useful to the government. Secretary of Defense Ash Carter said in a 2015 speech that attribution of cyberattacks has improved “because of private-sector security researchers like FireEye, Crowdstrike, HP—when they out a group of malicious cyber attackers, we take notice and share that information.” Moreover, private companies’ attributions ensure that foreign governments are accused of bad behavior, without the U.S. government having to do the accusing and bearing whatever diplomatic costs might follow.

But aside from these apparent benefits, reliance on private attributions to the exclusion of governmental accusations could be problematic for the U.S. government going forward.

First, the speed and detail of private companies’ attributions can make the government seem slow and overly cautious. This perception is heightened when government sources anonymously confirm to journalists that the government believes a foreign state is behind an attack—as government sources have with respect to the DNC hack—but the government continues to refrain from an official attribution. The absence of an official attribution may tend to foster ongoing questioning about the source of intrusions.

Another risk is that private companies are shaping expectations about the evidence needed for attributions. Think of this as a “CSI effect” whereby the portrayal of high-tech forensic investigation on television shows like CSI causes jurors in actual criminal trials to have unreasonable expectations about the amount and nature of evidence that should be presented. The cybersecurity equivalent is that private companies’ transparency about the evidence supporting their attributions of attacks to foreign governments may shape expectations about the evidence that the government should put forth when it makes similar accusations.

The “CSI effect” may have been at play in response to the FBI’s attribution of the Sony Pictures hack to North Korea. The FBI initially gave a high-level description of the evidence supporting its attribution, but was met with skepticism from the security community. To address continued questioning, FBI Director James Comey
provided a somewhat more detailed description of the FBI's evidence a few weeks later. The prevalence of detailed private attributions may be setting expectations for attributions that the government cannot match without compromising sources and methods that it needs to preserve, and absent detailed evidence, its attributions may seem less credible to security researchers.

The evidentiary standards matter not just as between the private sector and the government domestically, but also between countries. There is not yet settled state practice about the nature or amount of evidence that a state should put forth in accusing another state of a cyberattack. The U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security—a group that includes the United States, Russia, and China, among other countries—touched on the evidentiary issue in passing in a 2015 report. The report notes that “accusations of organizing and implementing wrongful acts brought against States should be substantiated” (para. 28(f)). Substantiated how or with what type of evidence, the report doesn’t say.

The United States has an opportunity to shape evidentiary norms about attribution, but to do so, it will need to make official accusations. To be sure, the stakes are high for official attributions. They have to be right, and accusations raise expectations that the government will take other responsive actions, like imposing sanctions (as in the Sony case) or filing criminal charges (as the United States has done with respect to hackers linked to China and Iran).

But the stakes are also high if the U.S. government sits out public attributions. If the United States does not officially attribute state-sponsored cyberattacks and cedes the field to private companies or other states, it risks losing control of both the narrative about particular cyberattacks and the evolving evidentiary norms. Instead, the norms may be influenced by the practices of private companies, whose reports may create a baseline that governments will have difficulty matching, or they may be set by the practice of other countries that are more forthcoming about official accusations.

Especially in instances where cyberattacks involve important values, like freedom of expression or electoral integrity, the United States should find a way to make substantiated, public attributions. Silence carries its own risks.

CFR seeks to foster civil and informed discussion of foreign policy issues. Opinions expressed on CFR blogs are solely those of the author or commenter, not of CFR, which takes no institutional positions. All comments must abide by CFR's guidelines and will be moderated prior to posting.

Pingbacks
AMERICAN BAR ASSOCIATION

CYBERSECURITY LEGAL TASK FORCE
JUDICIAL DIVISION
SECTION OF SCIENCE & TECHNOLOGY LAW
CRIMINAL JUSTICE SECTION
INTERNATIONAL LAW SECTION
SECTION OF ENVIRONMENT, ENERGY AND RESOURCES
STANDING COMMITTEE ON LAW AND NATIONAL SECURITY
STANDING COMMITTEE ON TECHNOLOGY AND INFORMATION SYSTEMS

REPORT TO THE HOUSE OF DELEGATES

RESOLUTION

1 RESOLVED, That the American Bar Association urges federal, state, local, territorial and tribal legislatures and government agencies to provide the funding necessary to develop, implement, and maintain appropriate cybersecurity programs for the courts and to train court personnel on methods to counter threats and protect judicial information systems from cyber intrusions or data breaches.
REPORT

I. INTRODUCTION

This Resolution focuses on cybersecurity threats that affect the judicial system and may pose a risk to the fair and efficient administration of justice. It urges federal, state, local, tribal and territorial legislatures and government agencies to provide the funding necessary to develop, implement, and maintain appropriate cybersecurity programs for the courts and to train court personnel on methods to counter threats and protect judicial information systems from cyber intrusions or data breaches.

The ABA Resolution is based upon the recognition that adequate funding and training are necessary to protect the public’s interest in the integrity of the courts and the data they hold. Such funding and training should enable the courts to perform a number of important tasks, including the conduct of regular risk assessments of each court’s information security program; updates to security controls; continuous vulnerability monitoring; the development and testing of comprehensive incident response and business continuity/disaster recovery (BC/DR) plans; and the sharing of cyber threat information among the courts and the legal community.

Over the years, the ABA House of Delegates has adopted a number of Resolutions sponsored by the ABA Cybersecurity Legal Task Force and the Section of Science & Technology Law that address cybersecurity threats and urge organizations to follow best practices to address them. In addition, the ABA has adopted Resolutions that address threats within courthouses and are directed toward participants in the judicial system, and any actual or perceived threat that may impede or interfere with access to the justice system and are also a threat to the fair and efficient administration of justice. The ABA has not adopted any policy that addresses the need for funding to develop, implement, and maintain an appropriate cybersecurity program for the courts.

From a security perspective, the courts in recent years have provided resources for building security. For example, the National Center for State Courts (NCSC) has been in the forefront of courthouse building security—a number of highly-publicized incidents of violence in courthouses around the country focused attention on this problem and best practices have been developed to address it.¹ Now, as the courts modernize their information systems, adequate funding will be required to develop, implement, and maintain an appropriate cybersecurity program, assess the threats to those systems, and protect the volumes of confidential and sensitive data that the courts collect, use, store, and share.

¹ The NCSC has conducted extensive research on the causes and prevention of court building violence and published Steps to Best Practices for Court Building Security (“Steps to Best Practices”), available at http://www.ncsc.org/services-and-experts/areas-of-expertise/-/media/Files/PDF/Services%20and%20Experts/Areas%20of%20expertise/Emergency%20Preparedness/Security_Best%20Practices_%20Steps_to_Best_Practices.aspx. These best practices represent collaboration with the Center for Judicial and Executive Security (“CJES”) in St. Paul, Minnesota, and the administrative offices of the courts of several states. NCSC encourages the leadership of every court building to strive to achieve and maintain best practices in every area identified in their publication so that every person who works in or visits a court building may do so in the safest environment possible.
As with all organizations, courts must remain forward-looking in managing their cybersecurity program. The threat environment, operational requirements, and innovation are constantly changing. This requires regular assessments of cybersecurity programs, evaluations of the effectiveness of controls and deployed technologies, and adjustments where necessary to maintain a strong security posture. This process necessarily involves a review of funding needs for the security program and updated training.

This is a particularly urgent need for state courts, many of which report having insufficient security budgets. The 2014 Deloitte-NASCIO study emphasized that the cybersecurity landscape for state government is a complex and challenging one, and concluded that unless deliberate action is taken, budgets will continue to be a challenge as cybersecurity threats mount.²

ABA has been an active proponent of adequate court funding. This Resolution builds on the ABA Resolutions adopted over the past decade that urge governments to provide adequate funding for the courts to ensure their security. As cybersecurity threats grow, the need for adequate funding for the courts to address these risks becomes critically important.

II. COURT TECHNOLOGY INITIATIVES

Courts at the federal, state, and local levels are embracing a variety of new technologies; many courts have undertaken important initiatives to modernize their information systems, measures that are designed to facilitate access, openness and transparency, increase efficiency, and reduce costs. These initiatives are vitally important to the cause of justice because they can make the courts more accessible and affordable to a diverse body of litigants. The NCSC website provides a summary of technology developments in state courts over the past decade.³ Important federal and state court technology initiatives are highlighted below.

In the 2014 Year-End Report on the Federal Judiciary, Chief Justice John Roberts announced that the U.S. Supreme Court will launch an online case filing system in 2016.⁴ Once the system is implemented, all filings at the Court—petitions and responses to petitions, merits briefs, and all other types of motions and applications—will be available to the legal community and the public without cost on the Court’s website.⁵

**Electronic Case Filing and Case Management (CM/ECF)⁶**—The courts have deployed new technologies to automate the filing, acceptance, and retrieval of the vast inflow of litigation documents that reach the courts every day. More than 600,000 attorneys have filed case documents using CM/ECF, and they currently file electronically more than 2.5 million documents each month. This system is not limited to attorneys. By logging onto the Public

---

⁵ Id. at 9.
Access to Court Electronic Records (PACER) system, members of the public can instantly access and review federal court filings located in courthouses across the Nation.\textsuperscript{7}

\textbf{“Next Gen” CM/ECF}—The national roll out of the Next Generation of the CM/ECF has begun in the U.S. courts of appeals. It is designed to increase chambers’ and clerks’ office efficiency and, when fully implemented, will provide a single sign-on that will allow court users and attorneys to file and retrieve information in any federal court using the same login and password, greatly simplifying access to the system. Testing in district and bankruptcy courts will begin in 2015.

\textbf{Courtroom Modernization}—The federal judiciary has likewise modernized courtrooms to take advantage of technological innovations in exchanging information and ideas. Attorneys can rely on computer-assisted graphics, video, and other technological aids to introduce evidence and facilitate communications with judges and juries.

\textit{Video conferencing} of court hearings is used to save costs and improve security in some situations by eliminating the need to transport prisoners and making it easier to allow victims and child witnesses to testify. Judges use it to conduct hearings remotely.

\textbf{Computer-assisted legal research} has been integrated into the case resolution process. Courts now have access to extensive legal databases and can quickly locate relevant authority through search commands on desktop computers, tablets, and mobile devices.

\textbf{Integrated Workplace Initiative (IWI)}— While the impetus for the IWI was to reduce the judiciary’s real estate footprint, courts are creating a better and more efficient workplace environment by capitalizing on the flexibility that new and emerging technologies provide. IWI examines how court units work, researches work style changes, and identifies successful mobile working situations, for example, where probation officers work remotely in the field rather than in the courthouse.

\textbf{eVoucher}—An automated system for processing and managing vouchers submitted by lawyers appointed to represent indigents under the Criminal Justice Act was developed by the District of Nevada. Through a collaborative effort, the eVoucher system is being adopted for national use and shared with courts throughout the country.

Other systems are being developed to assist litigants, jurors, and members of the public, including:

- Online jury services support
- Centralized and automated payable processes
- Virtual self-help centers to assist self-represented litigants

Additional technology changes are expected in the coming years to enhance court services.

\textbf{Electronic Discovery}—Amendments to the Federal Rules of Civil Procedures have spurred the transformation of litigation through e-discovery.\textsuperscript{6} e-Discovery has resulted in the transfer of

huge amounts of confidential and sensitive data from companies and other organizations to the
courts, law firms, technology companies, and other third party outsourcing entities.

**Governments Are Going Paperless**—The federal government and the states are transitioning
from print-only publishing to either an environment in which legal materials, including judicial
decisions and legislation, are published in a mix of formats or one in which legal material are
published in electronic format only. To address these developments, the Uniform Law
Commission adopted the Uniform Electronic Legal Material Act (UELMA), a model state law
that provides for authentication of legal material, and preservation and archiving of this material
for the future. This transition creates an immediate need for all federal, state and local courts to
protect their electronic records. At the federal level, the Government Publishing Office (GPO)
is developing best practices for authentication of official documents.9

**III. TECHNOLOGY CHALLENGES**

**Sensitive Data at Risk**

Litigation often involves sensitive matters: criminal prosecutions, bankruptcy petitions,
malpractice suits, discrimination cases, and patent disputes may all lead to the collection
of confidential information that should be shielded from public view to protect the safety
of witnesses, the privacy of litigants, and the integrity of the adjudicatory process.10

--Chief Justice John Roberts, U.S. Supreme Court (2014)

With the opportunities presented by information technology come many challenges and risks that
the courts must address. As courts modernize many aspects of their operations, their information
systems are becoming interconnected and users are now able to access court services through the
Internet. In today’s digital world, threats to data and information systems are found almost
everywhere a computer, server, smart phone, thumb drive, or other electronic device is operating
(including the cloud). The proliferation of mobile devices and wireless technologies present
vulnerable points in the flow of sensitive data in computer networks. Services are provided and
documents are stored in the cloud. These developments present cybersecurity issues that must be
assessed and taken into consideration as the courts determine their funding requirements for
court security.

**Law Offices, Governments, and the Courts Are Targets of Cyber Attacks**

The recent highly-publicized data breaches of leading retail companies, health insurers, and
government agencies have caught the attention of the public, politicians, and law enforcement.

---

The indictment of a Russian national charged in the largest known data breach prosecution provides details of attack methodology used by hackers in several of the largest data breaches.\(^{11}\) A website that goes by the name “information is beautiful” provides a visualization of hundreds of the major data breaches over the past decade and serves as a useful resource to identify and learn about the massive data breaches that have affected the private sector and government.\(^{12}\)

Similarly, the courts have suffered data breaches. For example, more than one million driver’s license numbers and 160,000 Social Security numbers (SSN) were accessed in a data breach at the Washington State Administrative Office of the Courts’ website.\(^{13}\) Citizens booked at a city or county jail, or with a traffic case in a district or municipal court through 2012, or anyone with a DUI citation in the state going back to 1989, may have had their data compromised. The courts have since taken steps to enhance their online security.

It is believed that hackers launched a successful denial-of-service attack against the PACER system that shut down online access for several hours in January 2014.\(^{14}\) Also uscourts.gov and various other federal court websites around the country were affected. The U.S. Court of Appeals website in the Middle District of Florida was also not available for an entire afternoon; no one could file or retrieve documents. A spokesperson for the Administrative Office of the U.S. Courts suggested that the outage was the result of a malicious attack, and the European Cyber Army claimed responsibility in a Twitter message.\(^{15}\)

The Florida Department of Juvenile Justice (DJJ) reported the theft of a mobile device containing youth and employee records in January 2011. The Tallahassee Police Department (TPD) was responsible for investigating the theft. The device, which was stolen from a secure DJJ office, was not encrypted or password-protected as required by DJJ’s technology policy.\(^{16}\)

Both large and small law firms have been the target of hacker attacks in the U.S. as well as abroad. The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals (2013) provides details about the threat landscape of legal organizations. The FBI

\(^{11}\) United States v. Drinkman, et. al., No. 09-626 (JBS) (S-2) (D. N.J.) available at http://www.justice.gov/sites/default/files/opapressreleases/attachments/2015/02/18/drinkman_vladimir_et_al_indictment_comp.pdf (second superseding indictment); http://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states (February 18, 2015). "This case reflects the cutting-edge problems posed by today's cybercrime cases, where the hackers didn't target just a single company; they infiltrated most of the country's email distribution firms," said Acting U.S. Attorney John Horn in Atlanta. "And the scope of the intrusion is unnerving, in that the hackers didn't stop after stealing the companies' proprietary data—they then hijacked the companies' own distribution platforms to send out bulk emails and reaped the profits from email traffic directed to specific websites."

\(^{12}\) http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.


has issued warnings to firms and held a meeting in early 2012 with approximately 200 law firms in New York City to discuss the risk of breaches and theft of client data.17 A cybersecurity firm that helps organizations secure their networks against threats and resolve computer security incidents estimated that 80 major law firms were breached in 2011 alone.18

Hackers targeted law enforcement officers from 70 different U.S. law enforcement agencies.19 In August 2011 hackers associated with Anonymous and the disbanded hacktivist group LulzSec published 10 GB of personal data of law officers, including thousands of SSNs and dozens of bank account numbers. Security firm Identity Finder CEO Todd Feinman, who disclosed this breach, characterized it as a “staggering amount of personal data that could cause identity theft problems for years to come.”20

Privacy Violations—Personally identifiable information (PII) that can be used for fraud and identity theft is being collected and often stored unprotected, putting many Americans at risk.21 PII, including SSN, has been publicly available through court online filing systems, and even published on court websites. There is a vibrant market for these data, and the harm to individuals from identity theft has been well-documented. As just one example, on its website, the Internal Revenue Service (IRS) indicates that it “has seen a significant increase in refund fraud that involves identity thieves who file false claims for refunds by stealing and using someone’s Social Security number.”22

Data breaches of government agencies are occurring with alarming frequency. In the annual report on the Federal Information Security Management Act (FISMA), the Office of Management and Budget (OMB) stated that federal agencies reported nearly 70,000 information security incidents in FY 2014, up 15 percent from FY 2013.23 The Government Accountability Office (GAO) found that the number of reported information security incidents involving PII have more than doubled over the last several years.24

In a state government breach, about 1,500 computers in the Massachusetts Office of Labor and Workforce Development were infected with the computer virus that was designed to let an

---

19 http://www.pcmag.com/article2/0,2817,2390582,00.asp.
20 Id.
attacker take control of infected computers and transmit confidential information to the digital thieves.\textsuperscript{25} Personal financial information, including names, addresses and SSN of up to 210,000 unemployed Massachusetts residents may have been stolen in the data breach in May 2011. In March 2012 hackers from Eastern Europe illegally accessed a Utah Department of Technology Services (DTS) server containing patients' SSN and data on children's health plans. It is believed that a weak password lead to the breach of about 780,000 patient files of Medicaid claims.\textsuperscript{26}

Malware on a San Francisco utilities agency server lead to a data breach of customer names, account numbers, addresses, phone numbers and some e-mail addresses for 180,000 customers.\textsuperscript{27} The agency notified customers that hackers used an open port on an unsecured server to infect it with computer viruses. Improper disclosure of sensitive records is a frequent cause of data breaches. In the State of Texas, 3.5 million records were accidentally published online, including names, addresses, SSN, DOB, and driver's license numbers.

The problem of data breaches will only become more serious in the future as the courts receive increasing amounts of confidential and sensitive data, reflecting a growing trend in data analytics. The sensitive personal data being amassed by companies and governments is staggering. Inexpensive storage has enabled companies to collect and store large amounts of data, and data analytics is driving companies to retain it far longer than they would have if it were in paper. Litigation will reflect these trends, resulting in the presentation of large amounts of critical, highly-valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery.

Security is only as strong as its weakest link. Failed security has resulted in thousands of data breaches that have led to the loss or compromise of millions of personally identifiable records, as well as the theft of classified information, valuable intellectual property and trade secrets, and the compromise of critical infrastructure.\textsuperscript{28} In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper security planning and implemented appropriate security safeguards. The NCSC launched the eCourts 2014 initiative to raise awareness of cyber threats and educate court personnel about the steps they need to take to secure their information systems and sensitive data.\textsuperscript{29}

\textsuperscript{25} http://www.mass.gov/lwd/.
\textsuperscript{26} http://www.eweek.com/c/a/Health-Care-IT/Utah-Health-Care-Data-Breach-Exposed-About-780000-Patient-Files-189084.
IV. ABA POLICIES

Cybersecurity

The House of Delegates adopted Resolution 109 during the 2014 Annual Meeting, sponsored by the ABA Cybersecurity Legal Task Force and the Section of Science & Technology Law. Resolution 109 encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected. The Report that accompanies the Resolution identifies accepted frameworks and standards that can serve as a reference for developing, implementing, and maintaining an appropriately-tailored cybersecurity program.

Risk Assessment—Cybersecurity is based on a systematic assessment of risks that are present in a particular operating environment. Risk assessments are undertaken to identify gaps and deficiencies in a cybersecurity program due to operational changes, new compliance requirements, an altered threat environment, or changes in the system architecture and technologies deployed. The National Institute of Standards and Technology (NIST) recently published the Framework for Improving Critical Infrastructure Cybersecurity and mapped the Framework to other accepted security frameworks and standards.30

Risk assessments are the basis for the selection of appropriate security controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level. Administrative, technical, organizational and physical controls help ensure the confidentiality, availability, and integrity of digital assets. Such controls should be carefully determined, implemented, and enforced. NIST has published extensive guidance on the selection of controls for government systems.31

Due to the nature of the threat environment, certain activities in a cybersecurity program are ongoing. Continuous monitoring and log analysis are designed to provide data that can enable the early detection of threats. To maintain a proactive security posture, potential threats should be investigated and targeted attacks detected in advance or addressed as they occur. The objective is to address cybersecurity threats and risks in a timely, disciplined, and structured fashion.

Incident Response and Business Continuity/Disaster Recovery (BC/DR)—Incident response is the practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference. Fully developed and tested incident response plans and business continuity/disaster recovery (BC/DR) plans are components of a cybersecurity program. Organizations should be prepared if a cyber attack or data breach occurs or if an event interrupts their operations. Response plans, policies,

and procedures should be able to accommodate the full array of threats, not just data breaches. A cybersecurity incident that is initially handled under an incident response plan may cause a business interruption that requires implementation of business continuity procedures. GAO has recommended key management and operational practices to be included in policies for responding to data breaches of PII.\textsuperscript{32}

The NCSC has focused on the need for emergency planning and response.\textsuperscript{33}

As is the case with most organizations today, data, in electronic as well as hard copy form, have become the life blood of courts. Managing data and files has become an essential court function. [ ] court operations face the risk of disruption that can be caused by many kinds of disasters or emergencies, both man-made and natural. When a disaster disrupts a court’s data system, the court will be hard pressed to discharge even its most basic and essential responsibilities. Therefore, courts must develop plans not only to prevent disruptions to data systems to the maximum extent feasible, but also to recover such systems as soon and as effectively as feasible after a significant disruption occurs.\textsuperscript{34}

\textit{Court Security}

Resolution 106C, adopted by the ABA House of Delegates at the Annual Meeting in 2005, made comprehensive recommendations related to federal court security. This Resolution also made recommendations that related to both the federal and state judiciaries, including urging Internet vendors and government entities to voluntarily remove certain personal information about a judge upon request, urging federal and state government departments and agencies to assess security needs of the administrative adjudication programs within their control, supporting the creation of a National Clearinghouse on Federal and State Court Security to facilitate information sharing, and urging Congress to explore ways to assist state courts with enhancing court security. The Resolution expands the scope of ABA policy on court security to fully encompass state, local, and territorial courts, including urging state, local, and territorial legislative bodies and governmental agencies to adopt laws and policies providing for the development and funding of adequate judicial system security protocols and to take the necessary steps to minimize the impact of court-related violence.

The Resolution further emphasizes the importance of applying principles of judicial administration to court security by recommending that courts engage in a comprehensive review of each court’s respective judicial system security needs, create and regularly review judicial system security protocols that fulfill those needs, and seek the funding necessary to implement those protocols. The Resolution also encourages the development of resources to educate those who participate in the justice system how to identify potential security threats related to the administration of justice, and how to be effective first responders in the event of an incident of violence. This multi-faceted approach was designed to enhance court security for all participants, promote fair and impartial courts, and increase public confidence in the judicial system.

\textsuperscript{34} \textit{Id.}
Resolution 106C included nine resolved clauses pertaining to court building and judicial security in the federal courts. For example, it urges Congress and the Department of Justice Judicial Security Review Group to review changes to U.S. Marshals Service (USMS) procedures to determine whether security vulnerabilities have been remedied. The Resolution also urges Congress to enact legislation requiring the USMS and the Administrative Office of the United States Courts to consult on a continuing basis, and for Congress and the Department of Justice to consider amending existing laws to strengthen court building and judicial security. Resolution 106C also encourages Congress to include sufficient funds in its annual appropriations for the federal judiciary and the USMS so that existing and additional security measures can be fully and effectively implemented.

A 2004 U.S. Department of Justice Office of the Inspector General Report, Resolution 106C, and numerous congressional hearings led to significant changes that benefit the federal courts. The USMS established the National Center for Judicial Security (NCJS) in fiscal year 2008. The goal of the NCJS is to provide educational, operational, and technical functionality in the areas of security not only to federal courts but to all levels of state courts as well. The USMS also established a Threat Management Center within its Office of Protective Intelligence. The purpose of the Threat Management Center is to provide 24/7 response support and information sharing between the USMS and state and local entities. During the 2012 fiscal year the Threat Management Center investigated and analyzed 1,370 threats and inappropriate communications to those protected by the USMS.\(^{36}\)

**Court Funding**

Ensuring effective court security at the federal, state, and local levels is in many ways related to funding issues. The ABA has been an active proponent of adequate court funding. The Task Force on Preservation of the Justice System (Task Force), under the leadership of past ABA Presidents Stephen N. Zack and Wm. T. (Bill) Robinson III, convened high-profile symposiums, hearings, and programs on the issue of court funding, and sponsored two Resolutions in 2011 and 2013. The House of Delegates adopted Resolution 302 at the 2011 Annual Meeting. Resolution 302 urges state, territorial, and local bar associations to document the impact of funding cutbacks to the justice system and to publicize those impacts so that the public may be informed of the need to support their court systems. Resolution 302 also urges state, territorial, and local governments to provide stable and predictable levels of funding to justice systems. The Task Force also sponsored Resolution 10C which was adopted at the 2013 Annual Meeting. Resolution 10C urges legislative bodies and governmental agencies to adopt laws or policies to ensure full and adequate court funding. Resolution 10C also adopted the *Principles for Judicial Administration*, promulgated by NCSC and adopted by CCJ in an effort to assist courts in their efforts to restructure court services and secure adequate funding.

The introduction to the *Principles for Judicial Administration* states that “[j]udicial leaders have the responsibility to demonstrate what funding level is necessary and to establish administrative

---


\(^{36}\text{U.S. Marshals Serv., http:// www.justice.gov/marshals/judicial/.}\)
structures and management processes that demonstrate they are using the taxpayers’ money wisely.” Reflecting that responsibility, this Resolution urges courts to create and review judicial system security protocols on a regular basis. The author urges courts to be proactive in assessing the needs and effectiveness of their judicial security systems so that they may effectively communicate with appropriators and policymakers. As the commentary to Principle 18 explains, “[t]he court management team is in the best position to know what resources are needed to fulfill its constitutional mandate and how best to present and justify its needs for those resources.” The proactive assessment of security needs is not only a vital component towards effective communication with appropriators, but is also crucial to the preservation of courts as a separate and co-equal branch of government.  

Principle 22 directly addresses the issue of court security, stating that “[z]esponsible funding entities should ensure that courts have facilities that are safe, secure and accessible and which are designed, built and maintained according to adopted courthouse facility guidelines.” Courts must examine existing national standards, including the resources discussed above, to determine how best to implement principle 22 in their jurisdictions. Every individual who interacts with the court must have access to proceedings in a safe environment. Adequate court funding is a necessary component in this endeavor. Principle 23 focuses on the importance of technology to provide required security, stating “the court system should be funded to provide technologies needed for the courts to operate efficiently and effectively and to provide the public services comparable to those provided by the other branches of government and private businesses.”

V. ABA POLICIES—SUMMARY

This section provides a list of ABA policies related to cybersecurity, court security, and court funding, with a brief summary and citation for each policy.

Cybersecurity

In recent years, the ABA House of Delegates and Board of Governors have adopted several policies regarding cybersecurity and lawyers’ use of technology, and the proposed Resolution is consistent with those existing ABA policies. These ABA policies include the following:


Resolution 109, which was sponsored by the Cybersecurity Legal Task Force and the Section of Science & Technology Law, encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature

38 Id. at 15 (Principle 18 states “Judicial Branch budget requests should be considered by legislative bodies as submitted by the Judicial Branch.”).
39 See Principles for Judicial Administration at 4 ("Court leaders, whether state or local, should exercise management control over all resources that support judicial services within their jurisdiction.").
and scope of the organization, and the data and systems to be protected.

The Resolution and Report are available at:


* * *

Resolution 118, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco (August 2013)

This Resolution condemns intrusions into computer systems and networks utilized by lawyers and law firms, urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions, and makes other related recommendations.

The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf

* * *

Policy Adopted by the ABA Board of Governors (November 2012)

The ABA Board of Governors approved a policy in November 2012 comprised of five cybersecurity principles developed by the ABA Cybersecurity Legal Task Force.

The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf

* * *

Resolutions 105 A, B and C, Adopted by the House of Delegates at the 2012 Annual Meeting in Chicago (August 2012)

Resolution 105A amends the black letter and Comments to Model Rule 1.0 (Terminology), the Comments to Model Rule 1.1 (Competence) and Model Rule 1.4 (Communication), and the black letter and Comments to Model Rule 1.6 (Confidentiality of Information) and Model Rule 4.4 (Respect for Rights of Third Parties) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and confidentiality. Resolution 105B amends the black letter and Comments to Model Rules 1.18 and 7.3, and the Comments to Model Rules 7.1, 7.2 and 5.5 of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and client development.
Resolution 105C amends the Comments to Model Rule 1.1 (Competence) and Model Rule 5.5 (Unauthorized Practice of Law; Multijurisdictional Practice of Law), and the title and Comments to Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding the ethical implications of retaining lawyers and nonlawyers outside the firm to work on client matters (i.e., outsourcing).

The Resolutions and Reports are available at:

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105a.doc

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_105b.authcheckdam.pdf

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105c.doc

Court Security

Resolution 106C, Adopted by the House of Delegates at the 2005 Annual Meeting in Chicago (August 2005)

Resolution 106C made comprehensive recommendations related to federal court security. It includes nine resolved clauses pertaining to court building and judicial security in the federal courts.

The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/directories/policy/2005_am_106c.authcheckdam.pdf

Court Funding

Resolution 302, Adopted by the House of Delegates at the 2011 Annual Meeting in Toronto, Canada (August 2011)

Resolution 302 urges state, territorial, and local bar associations to document the impact of funding cutbacks to the justice system and to publicize those impacts so that the public may be informed of the need to support their court systems; and urges state, territorial, and local governments to provide stable and predictable levels of funding to justice systems.
The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/administrative/tips/Court%20Funding/2011%20Annual%20Resolution%20302.authcheckdam.pdf

Resolution 10C, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco, CA (August 2013)

This Resolution urges legislative bodies and governmental agencies to adopt laws or policies to ensure full and adequate court funding. It also adopted the Principles for Judicial Administration, promulgated by NCSC and adopted by CCJ in an effort to assist courts in their efforts to restructure court services and secure adequate funding.

The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/administrative/tips/Court%20Funding/2013%20Annual%20Resolution%2010C.authcheckdam.pdf

VI. CONCLUSION

This Resolution focuses on cybersecurity threats that affect the judicial system and may pose a risk to the fair and efficient administration of justice. Now, as the courts modernize their information systems, adequate funding will be required to develop, implement, and maintain an appropriate cybersecurity program, assess the threats to those systems, and protect the volumes of confidential and sensitive data that the courts collect, use, store, and share. This Resolution builds on the ABA Resolutions adopted over the past decade that urge governments to provide adequate funding for the courts to ensure their security. As cybersecurity threats grow, the need for adequate funding for the courts to address these risks becomes critically important. The adoption of this Resolution will enhance court cybersecurity and promote fair and impartial courts.

Respectfully Submitted,

Judith Miller
Harvey Rishikof
Co-Chairs, ABA Cybersecurity Legal Task Force

August 2015
Cybersecurity Whistleblowing Is Murkier Than You May Think

Renee Phillips and Shea Leitch, Corporate Counsel

October 10, 2016

How can your breach turn into a securities law violation? The answer may be "via whistleblower." More and more, corporate employees are reporting cybersecurity vulnerabilities to the U.S. Securities and Exchange Commission after not receiving satisfactory responses from managers about issues they raise. Companies with a strong internal reporting protocol may believe that they need not worry about missing a valid internal report. But organizations should not be so sure. Cyber whistleblowers may present themselves in ways that are virtually unrecognizable from a traditional whistleblower perspective. Recognizing a potential cyber whistleblower may require companies to appreciate nuances previously unanticipated by most internal reporting schemes.

Consider the following scenario. An IT employee approaches his manager. He expresses concern that his co-workers are not following appropriate cybersecurity practices. Specifically, he is aware that employees share passwords for certain systems. The employee knows that his co-workers do this for convenience, but he is concerned that doing so presents a risk to company information. Many managers would not recognize this as a potential whistleblower situation. However, this simple complaint may indeed form the basis for a whistleblower report. If the employee believes that the vulnerability is serious and puts consumer or company information in jeopardy, the employee may take this information to the SEC.

What does the SEC have to do with all this? It’s become a very attractive venue for whistleblowers to lodge complaints. The Dodd-Frank Wall Street Reform and Consumer Protection Act amended the Securities Exchange Act to create a bounty program that pays monetary awards to whistleblowers who provide original information about violations of securities law leading to enforcement actions with penalties over $1 million. Whistleblowers who provide qualifying tips receive monetary awards between 10 percent and 30 percent of any recoveries, including from related actions.

Cybersecurity weaknesses may form the basis for an alleged securities law violation because securities laws and regulations increasingly require protection of sensitive data. For example, the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule requires companies to protect consumer records through administrative, technical and procedural safeguards. Institutions are required
to develop and implement an information security program appropriate for the size, complexity, nature and scope of the financial institution's business. Under this rule, if a company fails to adopt adequate cybersecurity controls or procedures and the failures lead to the exposure of consumer personal information, the company may be found to have violated the Safeguards Rule and, in turn, securities law.

Returning to our example above, the company's failure to maintain an adequate password management protocol could be viewed as a failure to adopt and enforce adequate procedural safeguards under GLBA. In recent years, a robust password management procedure has come to be recognized as a fundamental cyber hygiene practice.

Unlike other types of corporate whistleblowing, cyber whistleblowing may fly under the radar until the whistleblower makes a report to the SEC. The concerns of cyber whistleblowers often arise during the course of normal job duties. Moreover, IT managers may not be aware of the SEC bounty program or that reports need to be elevated. Employees who feel that their valuable advice has not been accepted, and those who feel obligated to come forward out of a sense of civic duty, are increasingly aware of the SEC's prioritization of cybersecurity in its enforcement agenda—and the potential for monetary bounties. And cyber whistleblowers have begun to come forward.

The SEC began signaling its interest in cybersecurity procedures in 2011, when it issued cybersecurity guidance to financial firms. The guidance made clear that the agency considers cybersecurity to be an issue critical to the integrity of financial markets, and advised companies to disclose material cybersecurity risks to shareholders. Since then, the SEC has conducted two examination sweeps aimed at evaluating the cybersecurity posture of financial firms.

At that point, the financial industry saw the writing on the wall. Cybersecurity enforcement actions were an inevitable reality, which came to fruition in September 2015, when the SEC announced the entry of its first consent decree in *In re R.T. Jones Capital Equities Management*. The commission alleged that R.T. Jones, the St. Louis-based investment company, failed to protect its customers' personal information by neglecting to conduct periodic risk assessments, employ a firewall, encrypt personal information and maintain a cybersecurity incident response plan in violation of the GLBA Safeguards Rule.

Around the time that the SEC announced the R.T. Jones enforcement action and consent decree, senior SEC leaders went to Silicon Valley to let tech leaders know that they were not hidden from the agency's watchful eye. Thus, for both nonfinancial public companies and financial companies, the SEC is determined to take a more active regulatory approach, and cybersecurity is high on the enforcement agenda.

But companies need not fear cyber whistleblowers. Organizations can implement simple procedures designed to acknowledge employee concerns and encourage them to report internally.

First, companies must make internal reporting mechanisms available and readily accessible. Employees should be able to report issues, including anonymously, to managers, human resources, compliance, ethics and legal. And they should be able to do so using a telephone, an email hotline or the company's website. Such reporting mechanisms should be made highly
visible, and employees should be encouraged to use them when appropriate circumstances arise. Employee handbooks and codes of conduct should explain why it is important to report concerns, and why the company encourages it. Managers should be trained to identify potential whistleblower situations, and to escalate employee concerns in an appropriate way.

Second, companies should safeguard the confidentiality of the whistleblower to the extent possible. Company policies should explain that reports will be treated as confidentially as possible, consistent with the business’s need to conduct a proper investigation. For anonymous reports, this means resisting the urge to try to identify the whistleblower. It is very difficult to retaliate against a whistleblower when nobody knows who that individual is. For non-anonymous reports, investigators should nonetheless avoid doing anything to unnecessarily "out" a whistleblower, such as identifying the employee in witness interviews or in document preservation memos. And they should be told not to ask witnesses in an investigation whether they are SEC whistleblowers. The SEC takes the position that employees are not required to inform their employers whether or what they have reported to the SEC.

Third, employee handbooks and codes of conduct should contain anti-retaliation provisions that make clear the organization will not tolerate any adverse action against an individual due to his or her good-faith report of wrongdoing. The policy should direct employees to report any potential retaliation to HR or Legal, and should explain that anyone found to have retaliated against an employee could be subject to discipline up to and including termination. Companies should also appoint an independent representative from Legal or HR to review employment decisions involving a whistleblower, including performance reviews, before they are finalized to ensure that they are not retaliatory and won’t expose the company to legal risk.

This is not to say that once some-one "blows the whistle" they are immune from employer discipline. But because of the increased risks involved, it is important to have independent review of management decisions involving whistleblowers.

Finally, companies should review their third-party vendor practices (contractors, consultants, auditors, hotline administrators) to ensure that they, too, contain optimal whistleblower procedures. Companies should also ensure that their own policies clearly encourage third-party reports.

Cybersecurity whistleblowing is an emerging area fraught with potential pitfalls. By creating a trusting environment for whistleblowers to report internally, a company can go a long way toward uncovering and remediating violations of law quickly and effectively. And when a company implements procedures designed to adequately address employee concerns and ensure that they feel that their complaints are heard, it may mitigate potential regulatory scrutiny.
the firm's whistleblower task force. Shea Leitch is an attorney in the firm's Washington, D.C., office and a member of its e-discovery and information governance group and cybersecurity and data privacy team.
PANEL IV:

REFUGEES, HUMANITARIAN CHALLENGES
AND THE LAW

MODERATOR:
ELISA MASSIMINO
Private Sponsorship of Refugee Resettlement in the United States:
Guiding Principles and Recommendations

October 2016
Acknowledgements

This report was written by Vasudha Talla, with the assistance of IRAP and Human Rights First. This report also benefited from extensive input from Kathleen Newland, Senior Fellow at the Migration Policy Institute. Finally, IRAP and Human Rights First also wish to thank the many individuals and organizations who provided helpful comments on various drafts of this paper.


Contents

Executive Summary ................................................................. 2
Private Sponsorship of Refugee Resettlement in the United States: Guiding Principles and Recommendations ................................................................. 4
   I. Private Sponsorship: Goals and Projected Outcomes ........................................ 4
   II. Background on Refugee Private Sponsorship Programs in the United States and Abroad ........................................................................................................ 5
   III. Legal Authority for Creation and Funding of a Private Sponsorship Program ......... 6
   IV. Ensuring that Private Sponsorship Does Not Displace Other Refugee Resettlement to the United States ................................................................. 7
   V. Refugees Admitted through Private Sponsorship Program Would Undergo Identical Processing and Screening as other Refugees........................................... 7
   VI. Models of Sponsor and Refugee Selection ......................................................... 8
   VII. What Would Private Sponsorship Entail? .......................................................... 11
   VIII. Overcoming Concerns Related to Private Sponsorship ..................................... 14
   IX. Recommendations for a Pilot Program ................................................................ 15
Afterword from Matthew La Corte, Niskanen Center ............................................. 17
Private Sponsorship of Refugee Resettlement in the United States:

Guiding Principles and Recommendations

Executive Summary

Overview: Individuals and organizations in the United States are seeking significant ways to assist refugees caught in the worst refugee crisis since World War II. There is fast-growing support for a private sponsorship program in the United States. Private sponsorship offers communities, organizations, companies, and philanthropies the opportunity to support the resettlement of additional refugees to the United States. Building upon the well-established model of the United States Refugee Admissions Program (USRAP)—a public-private partnership between the federal government and nonprofit resettlement agencies that successfully resettles thousands of refugees each year—private sponsors would be paired with refugees upon their arrival, providing financial support as well as cultural orientation and community integration. In the short-term, refugee families—especially those with special vulnerabilities—would enjoy dedicated attention and support from sponsors, while in the long-term, sponsors would expand the constituency of those invested in refugee resettlement and drive innovation in resettlement.

Legal authority to establish a private sponsorship program already exists. Under federal law, the president can determine the annual number of refugees to be admitted to the United States. President Reagan used this authority to launch the Private Sector Initiative, allocating 10,000 spaces for privately-supported refugees each year and facilitating 16,000 refugees’ admission during the program’s existence. A private sponsorship program must maintain the principle of “additionality”—i.e., any refugees who are resettled using private sponsorship should be in addition to refugees who are resettled using government funds rather than replacing government support. Other key aspects of a private sponsorship program should include:

Numbers: Within the annual Presidential Determination (PD) of the number of “government-sponsored” refugees to be admitted through USRAP, the president would establish a separate quota for “privately-sponsored” refugees—either as an absolute number each year, or as a percentage of the annual PD of “government-sponsored” refugees.

Selection and Matching of Refugees and Sponsors: The model for selecting refugees and sponsors in a private sponsorship program should accommodate the motivations of sponsors, while ensuring the resettlement of the most vulnerable refugees the efficient use of government resources. Three key models are: (1) matching a refugee already within existing priority streams of USRAP and pre-selected by the U.S. government or resettlement agency with a private individual or organization screened and approved by the U.S. government or resettlement agency, with no pre-existing relationship between the refugee and sponsor; (2) the U.S. sponsor names a refugee relative overseas, submitting an application to the U.S.
government for acceptance of the sponsor and refugee and contingent upon screening and approval; (3) the U.S. sponsor names a refugee overseas who they are not related to, submitting an application to the U.S. government for acceptance of the sponsor and refugee and contingent upon screening and approval. Sponsors could be required to: (i) live in certain states with robust benefits for refugees and/or organizations to train and monitor sponsors; (ii) undergo background checks; and/or (iii) provide proof of sufficient financial resources.

Privately-sponsored refugees would undergo overseas processing identical to that of all other refugees—i.e., they would be screened by relevant federal agencies to ensure that they legally qualify as a “refugee” and to verify admissibility. Privately-sponsored refugees would undergo the same multi-agency security checks as all refugees in USRAP.

**Sponsorship:** To ensure the principle of “additionality” and minimize the need for additional Congressional appropriations and government-funded benefits, sponsors would replace or cover government resettlement costs. Private sponsors could pay for pre-arrival costs through a combination of donations and fees to the U.S. Department of State, the U.S. Citizenship and Immigration Services, and other non-profit and international organizations involved in overseas processing. Post-arrival, private sponsors would be required to provide financial support for one year through a variety of methods. Sponsors could make in-kind donations (e.g., free housing); replace government benefits by directly providing refugees with cash assistance and benefits; and/or make tax-deductible donations to cover the cost of services best provided directly to refugees by government or resettlement agencies. After the private sponsorship term, refugees could enroll in means-tested benefits, if necessary.

In addition to financial assistance, sponsors would be responsible for cultural orientation and community integration, including initial reception, securing and setting up housing, assisting with the employment search, educational enrollment, and language classes, and providing information about the basics of living in the United States.

**Training, Oversight, Monitoring:** Adequate training, mentorship and monitoring is crucial to the success of a private sponsorship program. A resettlement agency or other organization would train sponsors on serving and supporting newly-arrived refugees. The organizations would serve as mentors and monitors—ensuring that the refugees’ needs are met, avoiding exploitation or abuse, and serving as a safety net should the sponsorship relationship dissolve. Sponsors could be required to provide a donation to the organization to cover training, monitoring, and other costs.

**Driving Innovation in Resettlement:** Private sponsorship could generate innovative models for private engagement in refugee issues. Private individuals, companies, and philanthropies could contribute to private sponsorship financially and logistically, even without being linked with a sponsored refugee. Municipalities and the private sector could establish group resettlement programs to fund the resettlement of groups of refugees in a particular area, with the possibility of special job opportunities. Educational institutions could sponsor resettlement for qualified refugees to continue their studies.
Introduction

Individuals and organizations in the United States are seeking significant ways to assist refugees caught in the worst refugee crisis since World War II. There is fast-growing support for a program allowing private sponsorship of refugee resettlement in the United States. Private sponsorship offers communities, organizations, companies, and philanthropies the opportunity to support the resettlement of additional refugees to the United States.

This white paper presents research and analysis of the key principles that should guide the creation of a private sponsorship program in the United States. It explores the considerations for various components of a private sponsorship program: legal authority for a program, selecting sponsors and refugees, funding, financial and other resettlement assistance, and sponsor training and monitoring. This paper proposes options for program design and concludes with recommendations regarding a pilot program that could be implemented in the short-term.

I. Private Sponsorship: Goals and Projected Outcomes

The United States Refugee Admissions Program (USRAP) is a well-established public-private partnership, with nine private resettlement agencies and hundreds of local affiliate organizations partnering with the federal government to resettle and integrate refugees in the United States.

While the growing global refugee crisis demands large-scale responses, the United States is constrained in its ability to resettle refugees, in part by limited Congressional appropriations for USRAP. The UN Refugee Agency (UNHCR) each year refers far more refugees to the United States for resettlement that USRAP can accommodate. Private engagement could supplement public funding and expand resettlement opportunities through USRAP. One possible solution—which has found long-standing success in Canada and has been implemented in countries such as Germany and Italy—is a private sponsorship program.

Private sponsorship in the United States should have two main goals. First, private individuals and organizations can facilitate the resettlement of additional refugees by providing both funds and critical support to refugees as they resettle in the United States, supplementing Congressional appropriations and integration services provided by resettlement agencies. Any system of private sponsorship should build upon the success and expertise of existing refugee resettlement agencies, and ensure that the addition of private resources does not decrease government support or overall refugee admissions.

Second, private sponsorship enhances and broadens support for refugee protection by directly involving private citizens in refugee resettlement. It would forge personal connections among individual Americans and resettled refugees, helping to dispel fears about
refugees and national security risks. It would increase private and philanthropic involvement in refugee resettlement by offering funding opportunities that are directly linked to additional refugee admissions. Private sponsors would become invested in refugee resettlement and refugee issues more broadly, creating a constituency that pushes Congress to increase funding and implement reforms. Sponsors can provide dedicated attention and support to refugees, including families with special needs, speeding self-sufficiency and heightening integration. A successful private sponsorship program in the United States may also benefit global refugee protection by encouraging other countries to increase resettlement through private sponsorship.

II. Background on Refugee Private Sponsorship Programs in the United States and Abroad

Private participation in refugee resettlement in the United States is not new. Throughout the 20th century, private organizations contributed to the costs of refugee resettlement, connected refugees with relatives in the United States, and assisted refugees with employment, housing, and integration. In the late 1980s, President Reagan created the Private Sector Initiative (PSI) and established a special quota for the admission of refugees who would be supported by private sector funding, in addition to those refugees supported by government funds. While 16,000 refugees were admitted through the PSI across five years, the program was discontinued in 1996 due to the steep and variable financial requirements for sponsors and a complex process for approving sponsors. Specifically, the health care costs of refugees, which could vary significantly between individuals and were difficult for a sponsor to anticipate in advance, became prohibitive.¹

Today, refugee resettlement in the United States is funded by the federal government and numerous non-profit resettlement agencies, along with state and local public service providers. The resettlement agencies receive arriving refugees and ensure that their daily needs—such as housing, food, household items, and other living expenses—are met for several months after arrival. Some resettlement agencies offer “co-sponsorship” programs, in which a group of individuals in the community is matched with a refugee or refugee family. Trained by the resettlement agency, the co-sponsors partner with agencies to provide housing and cash assistance, and help the refugees integrate into the community, including enrolling in school and finding employment. Co-sponsorship programs in their current form do not increase the total number of refugees admitted to the United States, but they do increase the capacity of local resettlement agencies to assist additional refugees, to expand the scope of services, and provide specialized attention to particularly vulnerable refugees.

Private sponsorship programs—in which private individuals or organizations pledge to cover most or all of the costs of resettlement for a specific refugee or refugee family—currently exist or have been implemented for short periods of time in Canada, Australia, Germany, and Italy, and are being considered in a number of other countries. Established in 1979, Canada’s private sponsorship program has allowed Canadians to offer new homes to 275,000 refugees. The Canadian program operates on two main principles, “additionality” (privately-sponsored refugees are over and above the refugees resettled and funded by the government) and “naming” (sponsors can propose the individual refugees they wish to sponsor for resettlement, although they are not required to do so). A 2007 government study of the Canadian private sponsorship program noted that, for a variety of reasons, privately-sponsored refugees became self-supporting more quickly than government-supported refugees, though the long-term earnings of both groups became roughly equivalent over time.\(^2\) Alongside the successes of the private sponsorship program, the Canadian government-funded program remains important.

III. Legal Authority for Creation and Funding of a Private Sponsorship Program

A private sponsorship program can be established using the existing legal authority over refugee screening and admission vested in the Executive Branch. Pursuant to the Refugee Act of 1980, the president has authority to determine and establish the annual number of refugees to be admitted to the United States. In fact, the Act requires the Office of Refugee Resettlement (ORR) within the Department of Health and Human Services (HHS) to incorporate the availability of private resources in its assessment of resettlement policies and strategies. Using this authority, President Reagan established the Private Sector Initiative, allocating 10,000 spaces for privately-supported refugees in addition to the refugees resettled and funded by the federal government.

Mechanisms currently exist that would allow private sponsors to cover various costs of processing and providing services to privately-sponsored refugees, perhaps assisted by philanthropic contributions from foundations, corporations, or private individuals. For example, the three federal agencies that carry out refugee screening and resettlement—the Department of State’s Bureau of Population, Refugees, and Migration (PRM), the Department of Homeland Security’s U.S. Citizenship and Immigration Services (USCIS), and ORR in HHS—could choose to accept gifts or set fees that cover the overseas processing and resettlement costs associated with privately-sponsored refugees. Fees and donations from private sponsors could be used to hire additional personnel to conduct overseas processing, or to fund the resettlement benefits issued by ORR to resettled refugees. International partners such as UNHCR and the International Organization for Migration (IOM) could accept donations from

private sponsors to cover expenses such as pre-departure medical exams that are otherwise funded by the federal government.

However, agencies that carry out security and background checks, including the FBI, National Counterterrorism Center, and Defense Intelligence Agency, are unlikely to set fees or accept gifts to augment their funding. The cost of security checks for privately-sponsored refugees would require funding through increased Congressional appropriations or internal reallocation of existing agency resources. Unless the costs of privately-sponsored refugees are covered through private sources or increased Congressional appropriations, the addition of privately-sponsored refugees to USRAP could increase backlogs and delays in USRAP.

IV. Ensuring that Private Sponsorship Does Not Displace Other Refugee Resettlement to the United States

Any private sponsorship program in the United States should maintain the principle of "additionality"—that is to say, any refugees who are resettled using private sponsorship should be in addition to refugees who are resettled using government funds. Additionality ensures that one major goal of a private sponsorship program is achieved—admitting more refugees to the United States—and avoids the possibility that private support for refugee resettlement displaces government support.

Additionality could be achieved by the president establishing a separate quota for "privately-sponsored" refugees in addition to the annual Presidential Determination (PD) of the number of "government-sponsored" refugees that are currently resettled through the USRAP program. For example, the PSI established by President Reagan established a special quota for privately-sponsored refugees that would be used only if private funds were made available to support these refugees. The quota of "privately-sponsored" refugees could be set as an absolute number each year, or as a percentage of the annual PD of "government-sponsored" refugees. As support for a private sponsorship program grows, the percentage method would link an increase of the "privately-sponsored" quota of refugees to an increase in "government-sponsored" refugees. Further, it could sidestep the concern that an increase of the "privately-sponsored" quota would be accompanied by a decrease in the "government-sponsored" quota.

V. Refugees Admitted through Private Sponsorship Program Would Undergo Identical Processing and Screening as other Refugees

Overseas processing of refugees admitted through a private sponsorship program would be identical to processing for refugees admitted through USRAP currently, except that the costs of resettlement of "privately-sponsored" refugees would be borne by the private sponsors and other private supporters of the program.
Refugees could be referred through existing priority streams and referred to PRM. (The program could later be expanded to include broader categories of family reunification, or to allow sponsors to propose refugees to be admitted based on family ties or other community-based ties.) Privately-sponsored refugees would be screened by USCIS to ensure that they fall within the definition of a “refugee” under U.S. law and to verify admissibility. They would undergo the same multi-agency security checks as all refugees in USRAP. Upon successful processing through USRAP, a privately-sponsored refugee would be admitted as a refugee to the United States and thereafter paired with their private sponsor for further resettlement assistance.

VI. Models of Sponsor and Refugee Selection

Several possible models for selecting sponsors and refugees in a private sponsorship program exist, some of which are used by private sponsorship programs in other countries and some of which draw upon the existing streams of refugees currently in USRAP. Each model reflects different interests and priorities. The model(s) chosen for a private sponsorship program should accommodate the motivations of sponsors, while ensuring the efficient use of government resources and that the humanitarian objectives of refugee resettlement are fulfilled.

1. Organization or Individual Sponsor “Matched” with Pre-Selected Refugee:

In this model, a sponsor would be matched with a refugee already within existing priority streams of USRAP and pre-selected by the U.S. government or resettlement agency to participate in private sponsorship. This is similar to the Canadian Blended Visa Office Referral program, and to co-sponsorship programs currently operated by U.S. resettlement agencies. The U.S. “sponsor” could consist of a group of individuals or an organization (church, synagogue, nonprofit, etc.) that demonstrates the ability to provide logistical and financial support, is screened and approved by the U.S. government or resettlement agency, and is trained by that agency.

By matching sponsors with refugees that have already been selected and screened by the U.S. government, this model would ensure that individuals will not be rejected by USCIS for not meeting the legal definition of a “refugee.” Further, sponsors would be matched with refugees slated to arrive to the United States in the short-term. Sponsors would not have to bear long processing delays before the refugees arrive, during which time sponsors may lose interest or financial resources. This model also facilitates private sector engagement between resettlement agencies and individuals or organizations not already involved in refugee issues.

This model could facilitate increased resettlement of refugees that face protection challenges or other vulnerabilities that warrant resettlement. Particularly vulnerable refugees, such as unaccompanied minors, torture victims, or single adults, whose psychosocial or financial needs are not currently met, could be matched with private sponsors who are
interested and willing to provide this support. A private sponsorship program, once well established, could fill gaps in benefits and services for these particularly vulnerable groups.

However, this selection and matching model, used alone, would not accommodate private sponsors who wish to sponsor a particular refugee that they know, motivated by a pre-existing relationship with that person or a desire to assist particular groups of refugees. Further, sponsors may have little lead time to establish a relationship with the sponsored refugee and may have limited information available to them about the refugee before his or her arrival to the United States.

(2) **Sponsor “Names” Refugee who is a Relative:**

Under this model, the U.S. sponsor is a relative of a particular refugee abroad. The sponsor can possess any type of legal immigration status in the United States and may have entered the United States in any way (i.e., as a refugee, as a visa holder, as a permanent resident). The familial relationship between the sponsor and refugee should allow sponsorship of married and adult children, siblings, uncles/aunts, nephews/nieces, cousins, and grandparents/children. Sponsors and refugees would submit a joint application to the PRM and/or USCIS requesting approval of the private sponsor and admission of the refugee into USRAP. To avoid the naming of individuals who are unlikely to fall within the definition of refugee under U.S. law, a refugee could be required to provide documentation that he or she has been recognized as a Convention refugee by UNHCR or a national government, or qualifies as a refugee under U.S. immigration law.

Family links between a sponsor and refugee can enhance resettlement and integration outcomes. Further, sponsors that are related to the refugees are likely to maintain their interest in sponsorship despite lengthy screening and processing times in USRAP. Should family sponsors not possess sufficient financial resources for the sponsorship themselves, they could partner with community-based groups or other organizations to serve as sponsors.

Family relationship should not, however, be the only criterion for eligibility for private sponsorship. Used alone, this model would exclude refugees that do not have family members in the United States to serve as sponsors, as well as refugees who may be unable or afraid to take advantage of family ties (e.g. LGBTI refugees). Family relationships could also be drawn too narrowly, and indeed a model based upon family relationships between the refugee and sponsor must acknowledge and accommodate a broad definition of family relationship in order to avoid the issues that led to the suspension of the P-3 stream in USRAP (fraud concerns, delays in DNA testing, etc.). Eligible family members would have to meet the definition of a refugee under U.S. law, in order to avoid USCIS rejection and inefficient use of government resources. Finally, if family links are required for private sponsorship, private engagement may not be forthcoming from new sources of civil society and private actors.

(3) **Organization or Individual Sponsor Proposes or “Names” Refugee:**
Under this model, the U.S. organization or individual sponsor can propose or “name” a specific refugee or refugee family it wishes to support, with no requirement of a family relationship between the sponsor and refugee. Sponsors and refugees would submit a joint application to PRM and/or USCIS requesting approval of the private sponsor and admittance of the refugee into USRAP. As with family members, a refugee could be required to provide documentation that he or she has been recognized as a Convention refugee by UNHCR or a national government, or qualifies as a refugee under U.S. immigration law.

This model would facilitate private sector engagement by individuals and organizations that are motivated to resettle a particular refugee or group (e.g., LGBTI refugees). Further, by allowing refugees to be proposed by sponsors, the model provides a pathway to resettlement for individuals who are unable or afraid to seek assistance from UNHCR or the government agencies that serve as the usual method of entering USRAP.

Possible disadvantages of this model could include the possibility that sponsors without a family relationship to the refugees may lose interest or financial resources over the course of the lengthy USRAP process. In addition, there is the potential for fraud or exploitation by middlemen who request payment from refugees in order to introduce them to a U.S. sponsor.

(4) **Sponsors Providing Financial Support Only:**

Private individuals already provide crucial financial contributions directly to resettlement agencies to support their work. For private individuals or organizations that wish to provide financial support to further a private sponsorship system, philanthropic donations could be directed to a “pooled” account held by a resettlement agency or other organization that would be used to fund privately-sponsored refugees at a local, state, or national level. Alternatively, a financial sponsor could be matched with a willing group of private sponsors to match the private sponsors’ raised funds or to provide the financial portion while the other private sponsors provide community support and integration. This could be particularly important in assisting private sponsors to cover major costs such as for overseas processing and screening, or for the health insurance costs of refugees.

(5) **Other Models of Public-Private Engagement and Sponsorship:**

A private sponsorship program could spur further innovation in refugee resettlement programs and increase private sector engagement. For example, municipalities and the private sector could establish a group resettlement program in which a group of refugees is funded and resettled together within a particular area or provided with special job opportunities. Another example is group sponsorship and resettlement through education institutions for qualified refugees.

* * * * * *
Building on the various sponsor-refugee selection models described above, further limitations and requirements could be included in a private sponsorship program. For example, sponsors may be required to live in particular states, such as those states with strong benefits and infrastructure to welcome and integrate refugees, those states with robust health care coverage available to refugees, and/or those states with local resettlement agencies that can provide training and oversight for private sponsors. In addition, sponsors may be required to undergo a background check or to provide proof of financial resources.

VII. What Would Private Sponsorship Entail?

Private sponsors would provide a range of resources, financial and otherwise, to the sponsored refugee. Depending on the model, private sponsors could contribute to pre-arrival processing and/or post-arrival resettlement costs. A private sponsorship program should fulfill the principle that “additional” refugees are resettled, while also ensuring that the need for additional Congressional appropriations and government-funded benefits are kept to a minimum. Estimates by other organizations of the cost of post-arrival refugee resettlement for the first year have ranged from $10,000 to $15,000 per person, not including Medicaid for those eligible.

Pre-arrival refugee processing: If federal agencies agree to utilize their gift-acceptance or fee-setting authorities, private sponsors could contribute to the costs of pre-arrival processing, carried out primarily by the Departments of State and Homeland Security. The cost of these activities can be established by reviewing Congressional appropriations to the relevant agency accounts and discussion with the agencies. Private sponsors (rather than resettlement agencies) could reimburse the federal government for some or most costs of pre-arrival processing:

1) Processing by the Department of State could be covered by making a tax-deductible donation, as the Department of State is authorized to accept gifts.
2) Processing by USCIS could be covered by a fee paid by sponsors. Alternatively, USCIS could cover its costs of refugee processing through a fee on other visa and benefit applications.
3) The costs of security screening, carried out by a variety of other law enforcement, security, and intelligence agencies that perform background and security checks, are not readily ascertainable and likely cannot be reimbursed by sponsors due to the many agencies involved and the confidentiality of the screening process.
4) Refugees' travel is arranged for and provided through a travel loan from IOM, which would still be provided to refugees and which sponsors, rather than the refugees themselves, could repay if they elected to do so.
Post-arrival refugee resettlement is funded, implemented, and overseen by the Department of State, ORR, and a network of nonprofit resettlement agencies throughout the country. Services that resettlement agencies currently provide include housing, furniture and household setup, cash assistance, transportation, clothing, English language classes, and employment services. Refugees also may receive federally-funded, state-administered benefits such as Medicaid, TANF, and SNAP food assistance, if they are otherwise eligible.

Private sponsors, along with private companies, philanthropic organizations, and other groups, could fund federal, state, and local services to refugees, and assume many of the costs and in-kind benefits provided by resettlement agencies. The cost of benefits and services from all sources can be established by reviewing Congressional appropriations to relevant agency accounts and discussion with resettlement agencies.

Private sponsors would commit to funding post-arrival services and benefits for one year, though sponsors would be encouraged to continue mentoring and providing community support in the long-term. Sponsors could continue providing financial support beyond one year if they so elected, but like the government-funded resettlement program, they should place a very strong emphasis on refugees achieving self-sufficiency within the sponsorship period. Research has shown rates of employment among refugees comparable or exceeding their U.S.-born counterparts, and sponsors should work to ensure that high rates of employment continue.

Private sponsors can fund post-arrival services and benefits through a combination of methods, including:

1. replacing certain government benefits. For example, the private sponsor would provide the refugee with funds so that refugee does not receive Reception and Placement funding from PRM or enroll in public benefits. While privately-sponsored refugees would remain legally eligible for means-tested benefits (such as food stamps), the sponsor would provide financial or in-kind support to exceed federal poverty guidelines and ensure that sponsored refugees did not need means-tested benefits for the sponsorship period;
2. providing in-kind donations such as free housing;
3. providing a tax-deductible donation to ORR or the U.S. Treasury that reimburses ORR and the federal government for the provision of benefits and services to the refugee, including additional ORR administrative and personnel costs;
4. providing a tax-deductible donation to the resettlement agency that covers the agency’s cost of identifying and training sponsors, monitoring, and other services; or
5. some combination of these methods, so that the sponsor directly provides certain benefits through direct funding or in-kind donations, supplemented by a tax-deductible

---

donation to resettlement agencies and/or ORR to cover services best provided by resettlement agencies or ORR. Funds committed by a private sponsor could be supplemented by corporations and philanthropic institutions giving grants or in-kind donations to expand assistance to both privately-sponsored and government-sponsored refugees as well as the host community.

After training and drawing upon the expertise of a resettlement agency or other organization, private sponsors would assist refugees in their integration in the United States. These activities would include:

**Reception and Placement** (obligation for one year)
(1) welcoming family upon arrival in United States;
(2) locating appropriate interpretation services;
(3) locating and securing affordable and appropriate housing;
(4) initial setup of housing, utilities, and basic necessities;
(5) providing transportation to facilitate services, health care, benefits, and employment;
(6) registering children and adults for documents and education;
(7) facilitating access to English language classes;
(8) facilitating access to health care and additional needs. Options include covering health care costs through purchase of an Affordable Care Act exchange plan or another private insurance plan, providing a donation to ORR for Refugee Medical Assistance (RMA) benefits, or making a payment to a government agency to reimburse the cost of Medicaid coverage. Further research would be needed to determine the preferred method to cover the expenses of refugee health care;
(9) providing information about cultural orientation on basics of living in the United States (laundry, grocery, shopping, banking, public transportation, etc.);
(10) providing assistance in locating employment and job interviews;
(11) providing cash assistance for incidentals; and
(12) coaching family on budget, building credit, and other financial literacy.

**Community Support, Mentoring, Civic Engagement** (obligation for one year, encouraged to provide long-term)
(1) community support and mentoring; English conversation; ongoing cultural advice;
(2) educational and job support;
(3) obtaining adjustment to legal permanent residence and assistance with possible family-based reunification; and
(4) citizenship classes and application, and voter registration.

Private sponsors could be required to submit a resettlement plan and budget, as well as proof of sufficient financial resources. Sponsors also could be required to submit a signed statement agreeing to supply the needs of the refugee family through cash and in-kind
donations at a level that places the family at a standard of living above that of food stamp recipients (e.g. $27,000 for a family of 3 people). Models for demonstrating sufficient financial resources are the Affidavit of Support required in I-130 petitions, or the resettlement plan used by the Canadian private sponsorship program. Alternatively, private sponsors could establish a trust account for the benefit of a particular refugee or refugee family, into which funds can be deposited.

Sponsors would be partnered with a resettlement agency or other organization (such as a university) that would serve as a safety net should the sponsorship relationship dissolve. Sponsors could be required set aside a fixed sum or percentage of money to be held for the benefit of refugee, pending the successful admission of the refugee into the United States. If the refugee is approved for travel and arrives in the United States, those funds would be progressively used and disbursed for the benefit of the refugee throughout the sponsorship term. If the sponsorship relationship dissolves, the agency would still possess the financial resources to support the refugee. If the refugee does not arrive in the United States, the funds would be returned to the private sponsor. Insurance could also be obtained to cover unexpected expenses or sponsorships that dissolve.

VIII. Overcoming Concerns Related to Private Sponsorship

A private sponsorship program provides exciting new ways for the private sector to engage with refugee issues. Private sponsorship should fulfill the principle of additionality as much as possible. The admission of privately-sponsored refugees should not be used as a way for the federal government to reduce the number of refugees otherwise admitted through USRAP.

Further, the availability of private funds to assist refugee resettlement should not be used to advocate for diminished Congressional appropriations for USRAP, ORR, or resettlement agencies, which are currently underfunded. Rather, funds from private sponsors should be used to augment the funding of overseas processing and USRAP, thereby alleviating backlogs by increasing personnel and facilitating interviews and background checks. Private sponsors may pledge sufficient funds so that the need for additional Congressional funding for privately-sponsored refugees is minimized and states and resettlement agencies do not bear additional, unfunded resettlement costs.

Accountability and monitoring of private sponsors will be a crucial component of a private sponsorship program. Private sponsors should be trained and overseen by resettlement agencies, given the agencies' decades of experience resettling refugees. The relationship between sponsors and refugees should be monitored, to ensure that the needs of vulnerable individuals are being met and to avoid any exploitation or abuse. Monitoring and evaluation of a private sponsorship program should include consultation prior to private sponsorship to allow for adequate information collection, as well as feedback from sponsors, refugees, and training and service agencies about strengths and weaknesses. Assessment of private
sponsorship should include a variety of indicators of integration outcomes and the actual cost of the program to government agencies and to private sponsors. Further, evaluation should assess the model for refugee selection that is chosen, and whether that model fulfills the objectives of the private sponsorship program.

IX. **Recommendations for a Pilot Program**

A pilot of a private sponsorship program should be implemented in a manner that tests and assesses the strengths and weaknesses of the key components of a full-fledged program. In the short-term, a pilot would channel additional funds into USRAP, and if successful, would build robust support among communities for launching an expanded private sponsorship program.

The needs of resettled refugees exceed current levels of government-funded benefits and services. Stakeholders such as ORR have expressed interest in targeted pilot programs that focus on particularly vulnerable refugees, such as unaccompanied minors, torture victims, or single adults, whose psychosocial or financial needs are not currently met. A private sponsorship program, once well established, could fill gaps in benefits and services for these particularly vulnerable groups. It is important to recognize that the current public/private model still requires ample community and private funding support to meet the needs that *all* refugees have that are beyond the scope of the current model.

A pilot can be used to test and establish some of the baseline requirements for refugees and sponsors, and to measure some of the costs of private sponsorship. A pilot that could be implemented in the short-term would have the following characteristics:

1. **Selecting Refugees for the Pilot**
   1. The U.S. government, in conjunction with the resettlement agencies, would select the refugees to participate in the pilot from refugees already at an advanced stage in USRAP. These refugees have already been vetted by USCIS and undergone the numerous necessary security and background checks.
   2. The pilot would be open to refugees of any nationality.

2. **Selecting Host Communities and Sponsors for the Pilot**
   1. Site selection should be based on a combination of the following factors: (1) welcoming state governments with strong benefits, infrastructure, and enthusiasm for refugee resettlement; (2) participation in and availability of Medicaid and ACA health insurance plans; (3) local resettlement agencies that can providing training and oversight; and/or (4) companies and other private sources of grants or in-kind donations that can provide additional support. A pilot program could be used to investigate the best way for sponsors to cover
healthcare costs, and to assess the average cost of health care to sponsors.

(b) States that have indicated their support for the refugee resettlement program include: New York, Connecticut, Rhode Island, Vermont, Pennsylvania, Delaware, Washington, Oregon, California, Hawaii, Colorado, and Utah.

(c) Sponsors would be identified and selected by resettlement agencies, drawing upon individuals and community groups that have shown interest.

(d) Sponsors would be trained, supervised, and monitored by resettlement agencies.

(3) Welcoming and Supporting Refugees

(a) Sponsors may be asked to provide a financial contribution to PRM and USCIS to cover pre-arrival processing costs. This could be provided directly by the sponsor or raised from voluntary community contributions.

(b) IOM travel loans will remain available to refugees in the pilot. Sponsors will have the option to pay for the travel of the refugee family.

(c) Sponsors would provide financial sponsorship for one year, though the means of doing so should be flexible in order to test different methods. While some sponsors may be able to demonstrate that they can finance all reception and placement benefits, cover community integration and mentoring services, and pay for or provide long-term integration and self-sufficiency support for one year, other sponsors can participate if other sources (such as companies) can provide cash or in-kind donations that cover state expenditures on behalf of refugees.

(d) Sponsors should provide a fixed monetary contribution to the partner resettlement agency or other partner organization. This sum is used to cover costs for training sponsors, benefits and services provided to the refugee through the resettlement agency, and costs related to monitoring and evaluation.

(e) Sponsors should ensure that sponsored refugees adjust status to legal permanent residents.

(4) Monitoring and Evaluation of the Pilot

(a) A robust evaluation process should be created prior to the start of the pilot to ensure that appropriate objectives are established and relevant data is collected throughout the pilot.

(b) Refugees should be involved in the evaluation process throughout their participation in the pilot and after the pilot concludes.
Afterword

Although the civil war in Syria and the resulting refugee crisis started many years ago, it first registered on our national consciousness in September 2015. This is when images of 3-year-old Alan Kurdi’s body, washed ashore after the boat carrying his family capsized, were broadcast to a horrified audience. Those tragic images served as a wake-up call for many Americans who began looking for ways to help refugees fleeing persecution, violence, and war worldwide.

The magnitude of the current refugee crisis—unprecedented in recorded history—has led many in the U.S. to push for ways to harness the tremendous goodwill of everyday Americans looking to do their part to help. The idea of private refugee sponsorship answers the question refugee advocates receive from Americans on a daily basis: how can I help?

Private refugee sponsorship offers individuals, communities, and charities the opportunity to support refugees in addition to those admitted under the federal cap. Thanks to IRAP and Human Rights First’s important new report, Private Sponsorship of Refugee Resettlement in the United States: Guiding Principles and Recommendations, the specifics for what such a program could look like are now clear.

Private refugee sponsorship offers a new platform to those who want to help those impacted by the current humanitarian crisis. It provides a more direct pathway of support and allows Americans to forge deeply personal connections with refugees. Moreover, such a program fosters a robust pro-refugee constituency, while increasing private sector and philanthropic involvement in resettlement. Such a program increases America’s capacity to resettle refugees and infuses new resources into our refugee programs.

IRAP and Human Rights First’s report serves a crucial new function in the effort to launch private sponsorship in America: it answers many hard questions about how exactly the U.S. could create such a program. For example, questions about strategies to set the private quota, the process to select both sponsor and refugee, what sponsorship would entail for post- and pre-arrival services, the structure of a pilot, and others are answered cogently in the report, drawing on the expertise of leading refugee authorities and the successful Canadian model of private sponsorship.

As announced in September, a refugee sponsorship pilot program is under consideration at the U.S. State Department. With this report, administration officials have a clear road-map to use for what a private refugee sponsorship pilot project should look like in 2017.

America’s tradition of openness, compassion, philanthropy, and freedom should compel policymakers to launch a private refugee sponsorship program to further improve our refugee
system and expand our ability to provide safe haven to those in need by relying on passionate and selfless Americans.

Harnessing the extraordinary power of the private sector is one of the great challenges refugee advocates face during this era of unprecedented global displacement; private sponsorship is the answer to this challenge and the critical next step in honoring America's remarkable history of empathy and charity.

Matthew La Corte
Immigration Policy Analyst
Niskanen Center
October 2016
## CONTENTS

Foreword by Ambassador Ryan C. Crocker ........................................... 1
Executive Summary ............................................................................. 1
The Numbers ....................................................................................... 6
Refugees Increasingly at Risk Across the Region ............................... 7
Lack of Basic Rights Protection for Refugees in the Region ................. 9
  Self-Reliance and Permission to Work ........................................... 9
  Detention, Registration and Freedom of Movement ......................... 10
  Education ....................................................................................... 10
Escape Routes Closed ....................................................................... 11
Lack of Effective Resettlement or Other Routes to Safety .................. 14
DHS Obtains Extensive Information on, and Rigorously Vets, Syrian Refugees ................................................................. 16
Understaffing and Backlogs Continue to Hamper the Already Slow U.S. Resettlement Process ...................................................... 19
Impact on Front-Line Refugee Hosting States and U.S. National Security Interests ................................................................. 25
Factors Contributing to Push Refugees to Europe ............................. 27
Resettlement of Women, LGBT, and other Vulnerable Refugee Populations ................................................................. 30
Recommendations for U.S. Leadership of a Global Initiative ............ 31
Addendum ......................................................................................... 35
Endnotes ............................................................................................ 37
Foreword by Ambassador Ryan C. Crocker

The Syrian refugee crisis is at a pivotal moment. More than 11 million people are displaced within Syria, a country that has been ravaged by escalating violence, aerial bombings, and terror. Many civilians have been stranded in besieged areas of the country, cut off from international assistance.

Large numbers of Syrian refugees are now living in Lebanon, Jordan, and Turkey, placing tremendous strains on those countries and their critical infrastructures—water, electricity, sanitation, health care and education. Stressing that the pressure of hosting so many refugees is impacting Jordan’s infrastructures and economy, King Abdullah II recently warned that his country was at a “boiling point” and that “the dam is going to burst.” The lack of sufficient international support, through aid and resettlement, is exacerbating these strains.

Last year more than 1 million refugees and migrants—about half of them Syrians—fled by sea to Europe, and NATO has now launched a mission to counter the smuggling operations that transport people to Europe’s shores.

This is a global crisis. It is a crisis that very much involves U.S. interests, and it is a problem that can only be successfully addressed if the United States leads. As detailed in Human Rights First’s report The Syrian Refugee Crisis and the Need for U.S. Leadership, the United States must lead a major global initiative to address the refugee crisis. The United States must significantly increase its own humanitarian assistance, development investment, and resettlement commitments in order to enlist other states to do more, and to effectively advance its foreign policy interests.

A bold initiative—one that includes significant increases in resettlement and aid—will advance U.S. national security by alleviating the strains on refugee-hosting states and safeguarding the stability of a region that is home to key U.S. allies. While the United States is the largest donor of humanitarian assistance, American leadership cannot be defined simply by how large a check we write. We must also lead by example, and our allies in the Middle East and Europe need to see that we are truly sharing in the responsibility of hosting refugees.

We must also address the backlogs and bottlenecks that impede processing for refugees undergoing the resettlement process, and for Iraqis and Afghans who have put their lives on the line to work alongside the U.S. military. Severe backlogs undermine the reputation of these U.S. programs and the country’s ability to meet its commitments to its allies and to refugee-hosting states, as well as its commitments to protect vulnerable refugees. Refugees are more rigorously vetted than any travelers coming to the United States. Addressing backlogs would not undermine security; in fact it would strengthen the effectiveness of U.S. processing.

U.S. leadership of this global effort will not only benefit U.S. interests, it will also advance American ideals. In times of global crisis, our country cannot afford to abandon its ideals. This country’s values are inscribed on the base of the Statue of Liberty. In the words of Emma Lazarus, “Give me your tired, your poor, your huddled masses yearning to breathe free.” Providing refuge
to the most vulnerable in need of protection is what has built our nation and made it a beacon of hope in a dark world. This is not a partisan issue, it is an American issue.

I have served under both Democratic and Republican administrations, and I understand the power of our long tradition of bipartisan support for protecting vulnerable people who flee persecution and tyranny, and yearn for the freedom that is central to who we are as a nation. America’s leadership in protecting and resettling refugees has benefited the world—and enriched this country.

Faced with the largest refugee and displacement crisis since World War II, it is time for America to stand up for its values and to lead again.

—Ryan C. Crocker,
former U.S. Ambassador to Syria, Lebanon, Iraq, Afghanistan, Pakistan, Kuwait
Executive Summary

We believe that America can and should continue to provide refuge to those fleeing violence and persecution without compromising the security and safety of our nation. To do otherwise would be contrary to our nation’s traditions of openness and inclusivity, and would undermine our core objective of combating terrorism.

Bipartisan group of former U.S. National Security Advisors, CIA Directors, Secretaries of State, DHS Secretaries, and Retired Military Leaders, December 2015

Poised to enter its sixth year in March 2016, the conflict in Syria has displaced more than 11 million people. About 4.7 million have fled the country, the vast majority to neighboring states. About 100,000 refugees and migrants—half of them Syrians—fled to Europe by sea in January and February 2016 alone. More than 3,800 perished at sea in 2015. This is a humanitarian disaster. The failure to effectively address the humanitarian crisis has spiraled into a threat to the stability of the region surrounding Syria, the cohesion of the European Union, and the national security of the United States. On February 11, U.S. Secretary of Defense Ashton B. Carter announced U.S. backing of a NATO mission to stop the smuggling operations that transport people to Europe’s shores, or to “stem this tide” as Secretary of State John F. Kerry said a few days later. With the outcome of the limited two-week “cessation of hostilities” in Syria in doubt, the conflicts within the country—and therefore the refugee crisis—offer no promise of abating.

According to the United Nations, there are more than 60 million people displaced in the world today—the highest numbers since World War II—and Syrians account for the greatest number of these uprooted people. In 2014 and 2015, the international community failed to fully meet appeals for humanitarian aid and resettlement for Syrian refugees. Without sufficient support, the strain on the frontline refugee-hosting countries—including Jordan, Lebanon and Turkey—increased sharply. Across the region, governments and relief agencies cut food assistance, access to medical care and other essentials, deepening the suffering of refugees, who are generally prohibited from working legally in these states.

In the absence of adequate responsibility-sharing by other countries, Jordan, Lebanon, and Turkey imposed restrictions that denied entry to Syrian refugees and made it more difficult for those who had succeeded in fleeing to neighboring countries to remain in the region. As the Syrian government’s Russian-backed attacks on Aleppo intensified in February 2016, tens of thousands of Syrians fled to the Turkish border, only to be barred from entering. At the same time, roughly 20,000 Syrian refugees have been stranded in a remote desert area at Jordan’s border, which has been largely closed to refugees during the last two years. Beginning in January 2015, Lebanon implemented border restrictions that generally bar Syrians and initiated onerous registration requirements for remaining in the country that most refugees cannot meet. Not only do such border restrictions violate international law, they leave some Syrians trapped in a war-ravaged country. Prohibitions on entry, stay, and work also push refugees to seek protection outside the region.

As conditions in—and access to—frontline countries has sharply declined, many Syrians have embarked on dangerous journeys to Europe.
More than one million refugees and migrants—about half of them Syrian—traveled by sea to Europe during 2015. While the continent is hosting far fewer Syrian refugees than the frontline states, the numbers are nonetheless significant, and the arrivals of refugees and migrants—along with the lack of responsibility-sharing, absence of orderly registration and security screening procedures, and the effort of right-wing extremists to exploit the issue—is creating conflict both within and between European countries.

After World War II, the United States helped establish an international system grounded in the shared conviction that people fleeing persecution should never again be turned back to face horror or death. And since then, the country has often been a leader on refugee-protection, and has been the global leader on refugee resettlement. In response to the Syrian refugee crisis, however, it has failed to lead. While the United States has been the largest donor to humanitarian appeals, a February 2016 “fair share” analysis by Oxfam concluded that it had contributed only 76 percent of its fair share to humanitarian appeals for the Syria crisis and only 7 percent of its fair share of resettlement places to Syrian refugees.

In September 2015, Secretary of State Kerry announced that the United States would resettle “at least 10,000” Syrian refugees during the 2016 fiscal year, a modest pledge given the scale of the crisis and the capacity of the United States. Then, in late 2015, following the terrorist attacks in Paris, the resettlement of Syrian refugees became the target of intense political debate. Some politicians and members of Congress pushed for a halt to resettlement of Syrian refugees, saying they questioned whether security vetting was adequate, and some even proposed shutting out all Muslims. Human Rights First researchers traveling in the region learned that this rhetoric was reverberating on the frontlines, sending the wrong message to U.S. allies in the region and to refugees themselves, some of whom gave up hope of waiting for resettlement and instead decided to head to Europe.

A bipartisan group of former U.S. government officials, including ones with national security and humanitarian expertise, called on the United States in a September 2015 letter to resettle 100,000 Syrian refugees, over and above the worldwide refugee ceiling of 70,000. Such a commitment would, they said, “send a powerful signal to governments in Europe and the Middle East about their obligations to do more.” Christian and Jewish faith leaders have also called on the United States to resettle Syrian refugees, as has the Bipartisan U.S. Commission on International Religious Freedom, stating that, “The United States must continue to live up to our nation’s core values.”

By leading an effort to resolve this crisis, the U.S. government would not only live up to its ideals; it would also advance its own interests. Ryan Crocker, former U.S. Ambassador to Syria, Iraq and Lebanon, has explained that, “A U.S. initiative to resettle Syrian refugees in the United States affirmatively advances U.S. national security interests. Increased resettlement and aid helps protect the stability of a region that is home to U.S. allies.” In a December 2015 letter to Congress, a bipartisan group of former national security advisors, CIA directors, secretaries of state, and Department of Homeland Security secretaries likewise pointed out that “resettlement initiatives help advance U.S. national security interests by supporting the stability of our allies and partners that are struggling to host large numbers of refugees.” They also pointed out that refugees “are vetted more intensively than any other category of traveler” and cautioned that barring Syrian refugees “feeds the narrative of ISIS that there is a war between Islam and the West.” They urged the U.S. government to reject
“this worldview by continuing to offer refuge to the world’s most vulnerable people, regardless of their religion or nationality.” A copy of their letter is attached as an appendix to this report.

In January and February 2016, Human Rights First conducted research on the conditions facing refugees in the region surrounding Syria and the progress of U.S. resettlement processing. Researchers gathered information through interviews and meetings in Jordan, Lebanon, Turkey and Egypt. Our findings, detailed in this report, include:

■ Syrian refugees are increasingly at risk, and suffer sharply deteriorating conditions, across the region. States have closed their borders, blocking civilians from escaping Syria, and imposed restrictions that make it difficult for many refugees living in the region to remain, prohibit most from working legally, and leave them in constant fear of detention and deportation back to Syria. These measures have also triggered a rise in child labor and early marriage of teenage daughters. In Jordan, half the refugee families have children as primary or joint primary bread-winners according to UNICEF. Under these conditions, many refugees cannot survive, much less rebuild their lives.

■ The lack of effective regional protection, exacerbated by the lack of assistance and insufficient orderly resettlement or visa routes for refugees, is driving many Syrians to embark on dangerous trips to Europe. Roughly half the refugees in Jordan were thinking of taking the dangerous trip to Europe given the lack of permission to work and insufficient assistance, according to a survey by CARE International. In Turkey primarily, and also in Jordan and Lebanon, we heard reports that refugees who had been struggling to survive for years in exile lost hope in waiting longer for potential resettlement and decided to instead take the dangerous trip to Europe.

■ The failure to adequately address the refugee crisis is harming U.S. national security interests, threatening the stability of frontline states bordering Syria and contributing to disunity in Europe. In Jordan, Lebanon, and parts of Turkey, the large number of refugees is straining critical infrastructures—water, sanitation, medical care, education and housing, as well as economic and job markets. This is a threat to regional stability that the international community has failed to alleviate through sufficient assistance, development investment and resettlement initiatives.

■ Turkey’s January 2016 announcement that it will allow Syrian refugees to work, if effectively implemented, will be an important step towards improving protection for Syrian refugees that should be replicated by other states.

U.S. resettlement processing centers and government agencies are working hard to try to meet U.S. goals for admitting Syrian refugees, and the number of Department of Homeland Security (DHS) officers interviewing Syrian refugees is increasing. Still, a range of factors related to the processing of U.S. resettlement and Special Immigrant Visa (SIV) cases are undermining American leadership and the ability of the United States to advance its humanitarian, human rights, and foreign policy objectives. Our findings on U.S. resettlement processing, detailed in this report, include:

■ U.S. pledges to resettle Syrian refugees have fallen far short of the necessary leadership, given the scale of the crisis, the overall resettlement needs—which exceed 460,000—and the impact of the crisis on U.S. allies, regional stability, and U.S. national security interests. With its pledge to resettle
10,000 Syrian refugees this fiscal year, the United States has agreed to take in only about 2 percent of the Syrian refugees in need of resettlement, which amounts to less than 0.2 percent of the overall Syrian refugee population of 4.7 million. This lackluster response has been particularly detrimental given the traditional U.S. role as the global resettlement leader.

- **The United States government obtains significant amounts of information about, and rigorously vets, Syrian refugees resettled to the United States, who come primarily from Jordan and Turkey where they have been struggling to survive for years.** This vetting is the most rigorous of any travelers to the United States. It entails multiple interviews and involves numerous U.S. and international intelligence and law enforcement agencies, including the National Counterterrorism Center, the Department of Defense, and Interpol, which have extensive databases on foreign fighters, suspected terrorists, and stolen, false, and blank passports from Syria, Iraq, and elsewhere. This vetting includes access to information provided by many other countries, including those in the region surrounding Syria.

- **U.S. resettlement processing continues to be hampered by some bottlenecks, backlogs, and staffing gaps, which undermine the United States’ ability to meet its humanitarian, protection, and foreign policy goals.** Despite significant U.S. efforts to step up resettlement processing, these backlogs and staffing gaps make it difficult for the United States to meet even its modest commitment to resettle 10,000 Syrian refugees. As of January 31, one-third of the way through the fiscal year, the United States had resettled only 841 out of the 10,000 Syrian refugees it pledged to resettle by September 30, 2016. Processing deficiencies include:
  - Backlogs due to insufficient DHS staff to review several thousand cases on hold in which no decision has yet been made
  - Backlogs due to insufficient DHS and security vetting agency staff and prioritization to conduct follow-up inquiries on both refugee cases and cases of Special Immigrant Visa applicants who worked for the U.S. military in Iraq and Afghanistan
  - Lack of space at the U.S. Embassy in Lebanon which has long impeded U.S. resettlement from Lebanon
  - Cuts in UNHCR funding that may limit its capacity to identify, review, and refer cases and lack of other avenues for referring refugee cases for resettlement
  - Insufficient capacity to expedite protection and resettlement for refugees facing imminent risks of harm, including LGBT refugees

- **Iraqi refugees and many Iraqis who worked with the United States military or other U.S. entities are also stranded in the region.** As of January 2016, more than 50,000 Iraqis, including many who worked for the U.S. military and government, are caught in a backlog. Many have been waiting years to be brought to safety in the United States.

While the resolution of the conflicts within Syria must occur before significant numbers of Syrian refugees can safely return home (and even then there will be many Syrian refugees who cannot safely return depending on the security, political and human rights realities on the ground as well as the nature of their past persecution), there is much that the United States and the international community should do to help Syria’s refugees.

Secretary of State John F. Kerry pledged $925
million in aid at the February 4, 2016 donor conference in London, the United States should pledge increased resettlement at a high level meeting in Geneva on March 30, 2016 and the United States will host a conference on the global refugee crisis in September 2016. However, as outlined in the full set of recommendations later in this report, the United States must lead a comprehensive global effort to successfully address the crisis.

In order to effectively lead, to press other states to do more, and to advance its foreign policy interests, the United States must significantly increase its own humanitarian assistance, development investment, and resettlement commitments. Specifically, the United States should:

1. Work with other donor states to fully meet humanitarian appeals and significantly increase U.S. humanitarian aid and development investments in frontline refugee hosting states. In particular, with Congress’ support, the administration should substantially increase both U.S. humanitarian assistance for Syrian refugees and displaced persons and U.S. development aid. The United States and other donors should expand and replicate initiatives that increase opportunities for refugees to work and access education, while also supporting refugee-hosting communities.

2. Champion the protection of the rights of refugees, including their right to work, access education, and cross borders in order to escape persecution. The U.S. president and secretary of state should redouble efforts to press states to allow refugees to cross borders to access international protection. The United States should also ensure that NATO actions, as well as any proposed “safe zone,” “no fly zone,” or similar endeavors, do not violate the human rights of refugees and migrants, including the right to flee persecution and seek asylum, and do not end up exposing civilians to dangers. UNHCR has cautioned that NATO’s mission—to “close off a key access route” to “stem this tide,” according to Secretary Kerry—should not “undermine the institution of asylum for people in need of international protection.” Efforts to block people from crossing borders to secure protection often instead push them—and the smugglers who profit off migration barriers and human misery—to find other, sometimes riskier, routes.

3. Substantially increase the U.S. resettlement commitment. For fiscal year 2017, the U.S. government should, in addition to resettling refugees from other countries, aim to resettle 100,000 Syrian refugees, a commitment more commensurate with both the American tradition of leadership and U.S. national security interests. This commitment would be miniscule compared to that of Jordan, Lebanon and Turkey, and would amount to just over 2 percent of the overall Syrian population hosted by these and other states in the region and only about 21 percent of the overall resettlement need, estimated to exceed 460,000. This commitment would still fall far short of the U.S. “fair share” level of 163,392. Still, it would help push other countries to increase resettlement, visa, and other humanitarian admission places for Syrian refugees.

4. Address staffing gaps to reduce backlogs and bottlenecks in resettlement and SIV processing. DHS should immediately increase staffing and resources to resolve the several thousand Syrian resettlement cases waiting their turn for review in “no decision” hold. Over the next year, DHS should also increase the size of its refugee corps to meet U.S. admissions goals, and assure cases are not delayed waiting for DHS interviews. In addition,
to prevent extended processing delays, the President should direct DHS and U.S. security vetting agencies to increase staffing and resources for SIV and resettlement cases. Congress should encourage and support increases in staff and resources. These backlogs undermine the reputation of these programs and the country’s ability to meet its commitments to U.S. allies, other refugee-hosting countries, and vulnerable refugees, including those facing grave risks due to their work with the United States. Addressing backlogs would not undermine security; rather it would strengthen the effectiveness of U.S. processing. It is certainly not in the security interest of the United States to have delays in security vetting, which would potentially put off the identification of a person who might actually pose a security threat.

5. Appoint a high-level assistant to the president charged with refugee protection. The world faces the largest refugee and displacement crisis since World War II. The president should appoint a high level official to ensure strong U.S. leadership of efforts—across U.S. agencies—to address the global refugee crisis, advance the protection of refugees at home and abroad, and coordinate effective and timely U.S. resettlement and SIV processing. This senior official should also map out a plan for effective transition of leadership on these matters to the next administration.

In the United States, the Syrian refugee crisis has—at least for the moment—fallen off the front pages. Yet its impact on people and the stability of key U.S. allies and refugee-hosting countries increases with each passing day, and year. It’s long past time for the United States to lead.

This report illuminates the challenges posed by the refugee crisis and explains how the United States, in conjunction with its allies, should tackle them.

---

The Numbers

Our world is facing a refugee crisis of a magnitude not seen since the Second World War ... We must not be taken aback by their numbers, but rather view them as persons, seeing their faces and listening to their stories, trying to respond as best we can to their situation. To respond in a way which is always humane, just and fraternal.

Pope Francis, September 2015 speech to the U.S. Congress

More than 11 million people have been displaced as a result of the Syrian conflict. About 6.6 million are displaced within Syria, and 13.5 million are estimated to be in need of humanitarian assistance within Syria. Another 4.7 million have fled to other countries. More than 2.6 million Syrian refugees have been registered in Turkey, which is hosting the highest number of Syrian refugees. More than 1.1 million are registered in Lebanon, which has prohibited the registration of any more refugees since May 2015. One out of four people in Lebanon is a Syrian refugee. About 635,000 Syrian refugees are registered in Jordan, though the Jordanian government has stated that as many as 1.4 million Syrian refugees are living in the country.¹ For Jordan, even using the more conservative estimate of registered refugees, this means that at least one out of every ten people in the country is now a Syrian refugee. Egypt hosts an estimated 120,000 Syrian refugees, and Iraq about 245,000. These countries also host refugees from other countries, including Iraqis, Sudanese, and Palestinians.

More than one million refugees and migrants have crossed the Mediterranean in an attempt to reach Europe in 2015, about 49 percent of whom were Syrians. UNHCR reports that since 2014, 7,452 people have died while crossing the sea in attempts to reach Europe. Refugees and migrants

---

HUMAN RIGHTS FIRST
have continued to take these dangerous trips to Europe, with more than 13,500 people arriving weekly during January and February 2016. During the first six weeks of 2016, more than 80,000 refugees and migrants arrived in Europe by boat, more than in the first four months of 2015. UNHCR reported that nearly 68 percent of January arrivals in Greece were women and children, a shift from last year, and 56 percent were Syrians.²

During 2015, humanitarian appeals for the Syria crisis were woefully underfunded. UNHCR reports that just under 50 percent of the appeals it made for refugees in the region went unfunded in 2015. UNHCR’s Syria Regional Response Plan for 2014 was also underfunded, with 37 percent of the need unmet. World Food Programme (WFP) appeals were also drastically underfunded in 2015. By the middle of 2015, financial shortages had forced the WFP to reduce its assistance to 1.6 million Syrian refugees in five countries.³

A major donor conference for the Syria crisis, held in London on February 4, 2016, led to over ten billion dollars in humanitarian and development “pledges” of assistance for the crisis.⁴ U.S. Secretary of State John Kerry pledged $925 million in humanitarian and development assistance from the United States.⁵ While this was an initial announcement of U.S. assistance, and is expected to be supplemented, the U.S. “fair share” estimate by Oxfam for 2016 is estimated to be $2.16 billion.

Refugees Increasingly at Risk Across the Region

As the sixth year of the Syria conflict approaches in March 2016, Syrian refugees across the region are increasingly vulnerable and at risk. Refugees who brought savings with them from Syria have long since depleted those savings as they struggle to survive in exile. With humanitarian appeals chronically underfunded, many of refugees’ basic needs have been left unaddressed year after year. The cuts in food assistance in 2015 had—as one aid worker in Jordan told us—a “domino effect” on refugee families, impacting not only their ability to eat but their ability to pay rent. More families are facing the risk of evictions. Some felt they had no choice but to withdraw children from school so that the children could work to help support their families. Based on poverty lines adopted by the hosting countries, as of December 2015, 87 percent and 93 percent of refugees were living in poverty in Jordan and Lebanon, respectively.

In Jordan, we heard—from both aid workers and refugees—reports of increasing child labor, early marriage, and fears of detention and deportation to Syria. The Jordanian government’s severe cuts in medical care for refugees left many Syrian refugees without critical medical assistance. In Jordan, poverty among refugees increased by several percentage points between 2013 and 2015. Not only are about 86 percent of refugees in urban areas in Jordan living below the poverty line, but 80 percent have resorted to “emergency coping mechanisms,” such as sending their children to work, returning to dangerous areas of Syria, or marrying off daughters early. In Jordan, a majority of working children in host communities work six to seven days a week, with a third working more than eight hours a day.⁶

In Lebanon, recent surveys found that 70 percent of refugee households are below the poverty line of $3.84 per person per day, a significant increase from 2014 when 50 percent were below the poverty line. Refugees in Lebanon told Human Rights First researchers that they were struggling to survive. In 2015, an estimated 55 percent of Syrian refugees in Lebanon were living in informal settlements, unfinished buildings, over-crowded
apartments or other substandard housing, a 15 percent increase from the year before. Severely vulnerable households doubled from 26 percent to 52 percent in one year. Aid workers reported that families in Lebanon were eating much less, children were working, and young girls in their early teens were increasingly being married off because their parents could no longer afford to feed all in the family. In Lebanon, many aid workers noted that the number of Syrian refugee "street children" appeared to have increased significantly. These street children engage in work including begging and street vending. In Jordan and Lebanon, negative attitudes towards refugees appear to have escalated over the last year or two. One aid worker described the environment in Lebanon as "hostile," a view echoed by refugees interviewed by Human Rights First. The number of Syrians deported is regularly reported on the Lebanese news. Aid workers in Jordan also reported more negative sentiments from Jordanians, who see their medical care and schools impacted by Syrian refugees. Aid workers and refugees report that Syrian refugee children are sometimes bullied or beaten in schools in Jordan. In Egypt, with the deterioration of the country's economy, refugees are increasingly viewed as threats to Egyptian jobs. To some in Egypt, Syrian refugees are viewed as security threats, while African refugees have long been the targets of racist and xenophobic harassment and violence. In Turkey, which we visited after the January 12, 2016 suicide bombing in Istanbul, there does not appear to be the same degree of negative sentiment towards Syrian refugees. Syrian refugees in Turkey amount to about 3 percent of the country's population, although they are much more heavily concentrated in particular areas. In addition, the social and political climate in Turkey, as well as official government attitudes, have favored generally welcoming attitudes toward Syrian refugees. In contrast, they constitute one out of every four people in Lebanon, and 9 percent to over 20 percent of the population in Jordan (depending on whether the calculation is based on the number of registered Syrian refugees, or the government's estimate).
Lack of Basic Rights Protection for Refugees in the Region

I have thought for a long time that a strategy that relies only on aid—which in any case is only reaching a minority of those who need it—is a mistake.

Syrian refugee interviewed by Human Rights First in Jordan

Across the region, Human Rights First researchers heard—again and again—that refugee-hosting states in the region have denied refugees the ability to work legally, that refugee children face tremendous barriers to education, and that refugees are facing increasing risks of exploitation, detention, and deportation in the face of increasingly harsh government policies and registration requirements. Without protection of their basic rights—including protection from return to persecution, protection from violence in the country of refuge, the ability to work legally, effective access to education, and freedom from arbitrary detention—refugees cannot safely remain and rebuild their lives in the region.

Self-Reliance and Permission to Work

Across the region, the lack of legal permission for refugees to work prevents them from supporting their families, undermines self-reliance, and places parents and children at risk of exploitation. Human Rights First researchers heard numerous reports that refugee families feared that a working adult would risk detention or deportation back to Syria if caught working. As a result many families made the difficult decision to send a child out to work so that the family could survive. In Jordan, half of families have children as primary or joint primary bread-winners, according to UNICEF. Those adults who do work are often vulnerable to exploitation, with employers sometimes refusing to pay refugees (who cannot complain as they are working illegally), vastly underpaying refugees, or hiring refugees to work in conditions that are unsafe.10

As the conflict approaches its sixth year, the persistent lack of work permission has left many families feeling that they have little choice but to travel onward to other countries where they will be able to support their families. A recent survey conducted by Care International in Jordan indicated that roughly half of refugees there were thinking of attempting the dangerous journey to Europe because they lacked a "future with dignity" without the ability to work or sufficient assistance. In Egypt, aid workers and refugees reported that the lack of work authorization leads refugees to believe they have no future in Egypt, prompting some to take the risky trip across the Mediterranean to Europe.

On January 15, 2016, the Turkish government announced that it would allow Syrian refugees to apply for work authorization. The measure is sweeping and contains relatively few limitations, some of the most significant of which are that it only applies after a refugee has been registered in Turkey for six months, and limits the number of Syrians in any given workplace to 10 percent—even in those areas of Turkey where Syrian refugees represent a high proportion of the local population. During our visit in January 2016, aid workers and refugee advocates in Turkey were cautiously optimistic about the development, which had not yet been implemented. Most refugees we spoke to expressed gratitude and relief at the prospect of legal work authorization, although the availability of jobs that will pay enough for refugees to support their families remains a significant challenge. On January 11, the British government announced that Jordan had agreed to allow Syrian refugees to apply for 4,000 work permits, 2,000 in the garment industry and 2,000 for agricultural jobs. In connection with
the February 2016 London Donor Conference on Syria, the European Union announced that it would review restrictive rules that have made it difficult for Jordanian exporters to take advantage of duty-free, quota-free access to E.U. markets, and nudge E.U. firms to invest in Jordan to create over one million jobs in the region.\(^{11}\)

**Detention, Registration and Freedom of Movement**

In Jordan, Turkey, Egypt, and Lebanon, Human Rights First researchers heard increasing reports of detention and refugees' fears of detention. In many cases, refugees have been—and many more fear they will be—detained if caught working illegally, or begging, and potentially returned back to Syria. In Lebanon and Egypt, where onerous registration renewal requirements have been imposed, refugees have also been detained for not complying with these new government requirements. In Lebanon, aid workers reported increases in raids, evictions, searches and seizures, leading some Syrian refugees to be thrown into detention. As a result, many Syrian refugees—especially men—feel that they are subject to arrest and detention. As one aid worker noted, refugees have no money, no food, no school, and now because they are viewed as "illegal," many are scared to leave their homes because they fear detention or deportation.

In Turkey, refugee advocates and aid workers expressed concerns about the government's increasing use of detention. In November 2015, the Turkish government and the European Union negotiated a controversial deal under which Turkey agreed to prevent irregular migration to Europe in return for nearly three billion USD in assistance for Syrians in Turkey, promises of visa-free travel for Turkish citizens, and a renewal of discussions about potential E.U. membership for Turkey. As of February 2016, the funds had not been delivered to Turkey. On November 27, 2015, Amnesty International in Turkey reported that 50 Syrian refugees were being held at an EU-financed detention center following their participation in a peaceful protest against their ban from entering Greece, and that some refugees had been beaten in detention. The organization's Turkey researcher stated that "[r]efugees in Turkey are increasingly facing arbitrary detention and forced return to Syria as the government punishes those it perceives as jeopardizing its lucrative E.U. deal." Refugee advocates told Human Rights First that by June 2016 the Turkish government plans to have 10,000 detention beds open for migrants and asylum seekers, in anticipation of large numbers being returned to Turkey by the E.U. starting in June 2016, under the portion of the E.U.-Turkey migration deal under which Turkey has agreed to readmit migrants and asylum seekers deported from the E.U.

**Education**

Across the region, aid workers and refugees report significant barriers to education for refugee children, teens, and young adults. In Egypt, Jordan, Lebanon, and Turkey some steps have been taken to open schools to younger children, and donors have invested in education for refugee children. In Jordan, for instance, many schools operate a second shift for Syrian children, with Jordanians going to school in the morning, and Syrian children attending in the afternoons. In Egypt, Syrian refugee children are permitted to attend the already overcrowded public schools. In Turkey, the government in 2014 took measures to remove legal barriers to school registration for Syrian refugee children, who are allowed to attend Turkish public schools or may instead attend privately-run "temporary education centers" for Syrian children that are now accredited by the Turkish government.
But a range of impediments keep many Syrian and other refugee children out of schools. A vast majority of school-aged Syrian children reside outside refugee camps in towns and cities. Although measures implemented in 2014 to facilitate school registration have improved enrollment, in Turkey, still only 25 percent of Syrian refugee children living in urban areas attended school in the 2014-2015 academic year. Many Syrian children who do enroll face difficulties in Turkish schools due to the fact that school is conducted in Turkish and that schools lack programs to teach students Turkish as a second language. A further problem in national public schools across the region is the lack of experience of those school systems in teaching children who have suffered war-time trauma. In addition, and across the region, there are not adequate remedial programs to teach Syrian children who, as a result of the conflict, have now been out of school for four years or more. As discussed above, many refugee children are working across the region, and as a result do not attend school. In turn, children who have been out of school for some time face particular difficulties in reintegrating in school in their country of exile and are particularly vulnerable to being driven into the workforce.

In Jordan, the government provides primary and secondary education free of charge for Syrian refugee children, but the many associated expenses—books, fees, transportation costs—make attendance at school impossible for many refugee children. In addition, in several countries in the region, aid workers and refugees have reported that refugee children face harassment or violence at schools, or in transit to and from school. School attendance for refugee children has actually declined in Jordan. In 2013, about 30,000 Syrian refugee children were out of school. This number rose steeply in 2015, with 90,000 Syrian children out of school in Jordan. Refugees have very little access to higher education. We spoke with a number of refugees whose higher educations and clearly planned career goals had been interrupted by the events that led them to flee Syria, and who were watching in despair as their futures disappeared. A lack of access to higher education in countries of first asylum is a disincentive for youth to complete secondary schooling, particularly in countries where refugees are also barred from legal employment. Some positive steps offer opportunities for replication, expansion and additional efforts. In Turkey, for instance, an initiative that offered 70 university scholarships for Syrian refugees prompted 5,000 applications. In Egypt, the government has allowed Syrian students to pay local tuition rates for university, but many are unable to transfer credits from Syrian universities as those schools are not considered accredited by Egyptian colleges.

**Escape Routes Closed**

*I fled Assad’s and Russia’s bombardment. Please tell them to open the doors so we can move to safety. We have no safety here.*

_Elderly Syrian woman, blocked from crossing to Turkey, February 2016*

In the absence of adequate responsibility-sharing by other countries, front-line refugee hosting states have imposed an array of restrictions, escalating in 2015, that block entry to many refugees trying to flee Syria. Turkey’s recent refusal to allow thousands fleeing the Aleppo attacks to escape across its border is one vivid example, but Syrians have been denied the right to flee their country on a daily basis at Syria’s other borders as well. Not only do border restrictions that improperly bar refugees violate international law, but they leave Syrians with no

---

**HUMAN RIGHTS FIRST**

611
New Lebanese Registration Requirements Impact Employment, Education, Detentions, and Protection

In January 2015, the Lebanese government issued regulations that require Syrians to pay $200 USD—per person—for an annual residence permit and sign a pledge not to work, or alternatively to find a Lebanese sponsor. Not only are the registration and renewal processes prohibitively expensive for refugees, but they are also so complicated, and require so much documentation, that most refugees cannot actually renew their registration. In some cases, families who cannot afford the costs, decide to have only the father renew his registration. In May 2015, UNHCR stop registering new refugees upon the demand of the Lebanese government. As a result thousands of Syrian refugees in Lebanon have not been registered, though UNHCR has recorded their information, including fingerprints and iris scans.

Without appropriate documentation, refugees in Lebanon cannot secure legal and physical protection. These new requirements limit the ability of refugees to register marriages and their children’s births (and could ultimately prevent children from securing Syrian citizenship, leaving them stateless), leave them vulnerable to exploitation, and increasingly subject them to detention and deportation back to Syria. A January 2016 Human Rights Watch report concluded that registration regulations left most refugees without legal status, often prohibiting their access to livelihoods, healthcare, education, and shelter as well as leading to a deterioration of refugees’ legal and economic status, increasing the burden on the host community.¹⁴

way out of a country ravaged by barrel bombs, conflict, and terror. These moves also make clear to many Syrians that they cannot secure effective protection in the region.

The countries that border Syria have legitimate security concerns, but they can address these concerns through individualized exclusion assessments conducted in accordance with international law. Blanket or random denials of entry violate the Refugee Convention and international law prohibitions against return. Drafted in the wake of World War II and in the context of the many border restrictions that denied refuge to those fleeing Nazi persecution, the Convention and its Protocol prohibit states from refoulement, or returning people to places where their lives or freedom would be at risk. Even states that are not party to the Refugee Convention and Protocol must comply with this prohibition as it constitutes a tenet of customary international law.

Jordan restricted entry to a number of categories of refugees fleeing persecution and conflict during 2013 and 2014, as documented in a December 2013 Human Rights First report and a 2015 Refugee Council USA report, to which Human Rights First contributed. For example, Jordan turns away single men, refugees who had traveled back to Syria (a refugee might, for example, return to retrieve a family member who is unable to travel alone), Palestinians formerly resident in Syria, Syrians without identity documents and Syrian refugees fleeing from areas of Syria controlled by ISIL. In mid-2014, Jordan all but
closed its borders to Syrian refugees, leading to a build-up of several thousand refugees stranded in a remote desert “no-man’s land” along the Syrian border. As a result of these border policies, the average number of arrivals in Jordan dropped from 60,000 per month down to around 10,000 per month between January and September 2014, and down even further to only several hundred a month at the end of 2014. In December 2014, the government allowed hundreds of Syrian refugees, including women and children, who had been stranded in the “no man’s land” to enter the country, though there were concerns that many may have been returned to Syria without being registered as refugees. Beginning in September 2015, as Syrians fled Russian airstrikes and ISIL terror, the number of refugees stranded in the desert and blocked from entering Jordan rose sharply. The numbers reportedly tripled between November and December 2015. As of January 2016, over 16,000 Syrian refugees were stranded on a berm in this remote desert area. By February, the number had reportedly climbed to 20,000. Jordan continued to allow in only very small numbers. On February 16 to 17 for example, Jordan reported that it allowed 82 Syrian refugees to enter Jordan. The weather in this desert area, where there is no water, has been described as “harsh,” and the conditions as “horrendous” by aid workers who have visited the area. In two weeks alone in early 2016, 70 to 100 Syrian refugees reportedly died from winter storms, war wounds, malnutrition, and disease. One aid worker estimated that there could be 40,000 refugees stranded in the desert by the summer if the situation is not resolved. The Jordanian government has repeatedly challenged the international community to take the refugees stranded at the border.\(^{15}\)

These refugees are overwhelmingly families, including elderly people and pregnant women, according to aid workers. The Jordanian government has said that some of the individuals at the border present security risks as they have come from areas controlled by ISIL; the government has also repeatedly stressed the financial pressures of hosting refugees and its need for additional aid from the international community. In January 2016, the Jordanian Prime Minister said “[I]t is true that supporting the Syrian refugees is our duty but we are doing this on behalf of the world ... If the world supports us, then we can keep our borders open and, if not, then how can Jordan, in light of its troubled budget, be able to serve them [refugees]?”

As noted above, the Jordanian government could implement fair and effective procedures for screening out individuals who present security threats and are not entitled to international protection, providing access to UNHCR. Moreover, there is also space in refugee camps within Jordan to hold these refugees.

Turkey too has closed its borders to Syrians seeking refuge. Turkey had periodically closed its borders during 2013 and 2014, but largely allowed Syrian refugees to enter the country until the end of 2014. In January 2015, Turkey imposed rules requiring Syrians to have valid travel documents in order to enter the country, a requirement that barred many legitimate Syrian refugees. In March 2015, Turkey announced the closure of two remaining border crossing points. Most recently, in early January 2016, Turkey imposed a new visa requirement for Syrians arriving by land or air. As a result of these policies, thousands of refugees have been prevented from escaping Syria, and many have been left with little choice but to turn to smugglers to try to escape the violence raging in Syria.

As Syrian government attacks on Aleppo and its surrounding countryside, supported by Russian aerial bombing, escalated in February 2016, tens of thousands of Syrians fled to the Turkish border, only to be barred from crossing to Turkey. About
58,000 people fled to the border area within a two-week period in February. Another 110,000 internally displaced persons were already living in camps at Bab al-Salama on the Syrian side of the border crossing. On February 9, 2016 UNHCR called on Turkey to "open its border to all civilians in Syria fleeing danger in need of international protection." On February 19, Amnesty International reported that Turkish authorities had denied entry to Syrian civilians in need of immediate medical care and that Turkish security forces had shot and injured civilians, including children who, out of desperation, attempted to cross the border with the help of smugglers.

Recent reports indicate that Turkish authorities are under pressure to stop refugees from heading to Europe and under growing pressure from the United States to secure the border more tightly because of the risk of militants travelling across borders. 16

Prior to 2015, refugees who were prevented from crossing to safety in Jordan or to a much lesser extent given the risks or impossibility of cross-country travel in Syria, Turkey could try to make their way to Lebanon. However, in January 2015 Lebanon imposed new border rules that have generally barred Syrians from escape to Lebanon. These rules include no exception for refugees and no exception for people fleeing persecution and war. This new policy is leading many refugees to be denied entry to Lebanon and turned back to Syria in violation of customary international law protections against refoulement. An extremely small number of refugees are allowed to enter Lebanon under a "humanitarian" entry category. The few examples include minors whose guardians are in Lebanon (and not the reverse), elderly or disabled people whose caregiver is in Lebanon, and individuals in need of life-saving medical care not available in their country. Over the last year, one aid worker estimated that only about 11 cases have met this "humanitarian" exception. Not only is this process extremely limited, but there is no effective process at the border to assess whether individuals should be let in or not. For instance, as of January 2016, the Lebanese Ministry of Social Affairs, which is responsible for making these determinations but is not the agency in charge of border security, did not have staff at the border to make these evaluations.

The Lebanese border rules include an exception for "transit" visas, so some Syrians have been able to escape Syria if they can show they are merely transiting through Lebanon. Many Syrian refugees did transit through Lebanon to Turkey, with some then heading onward to Europe. However, many Syrians will now be prevented from leaving Syria to transit to Turkey via Lebanon due to the new Turkish visa requirements. After these visa restrictions went into effect in early January 2016, Lebanon deported several hundred Syrians, who were planning to travel by plane to Turkey, from the Beirut airport back to Syria. As a result, yet another escape route for Syrians has been blocked.

---

**Lack of Effective Resettlement or Other Routes to Safety**

Resettlement can be a life-saving solution for vulnerable refugees who are struggling to survive in front-line countries that host the overwhelming majority of refugees. Resettlement is also a tangible demonstration of responsibility-sharing by countries outside the region, providing critical support to front-line refugee hosting states as they struggle under the strain of hosting large number of refugees. In addition, it can also be a tool for protecting other refugees—particularly if effectively leveraged—by encouraging front-line
countries to continue to host the bulk of refugees and to allow additional refugees to cross into their countries to escape conflict and persecution.

In September 2013, UNHCR launched a formal appeal for resettlement and other humanitarian admission slots for Syrian refugees, and in February 2014, the U.N. High Commissioner for Refugees called on states to provide 130,000 places for Syrian resettlement or admissions. Throughout 2014 and 2015, the High Commissioner repeatedly called on countries to pledge more resettlement or other admission spots for Syrian refugees. In a March 30, 2015 “fair share” analysis, Oxfam found that pledges still fell 55,890 below the 130,000 goal. It also concluded that the number of pledges fell 121,890 below the actual resettlement needs of Syrian refugees. As of June 2015, UNHCR reported that it was still 27,000 short of its 130,000 Syrian pledge goal. As global attention increasingly focused on the escalating number of Syrian refugees and others taking the dangerous journey to Europe, pledges increased in late 2015. Canada, for instance, committed to take in about 25,000 Syrian refugees.

UNHCR has estimated that about 10 percent of the Syrian refugee population is extremely vulnerable and in need of resettlement, though given deteriorating conditions, UNHCR has explained that the 10 percent target should be considered an important milestone rather than a final goal.17 As the registered Syrian refugee population has, as of February 2016, grown to 4.6 million (and by the end of February to 4.7 million), at least 460,000 vulnerable Syrian refugees are now in need of resettlement to third countries. In its 2016 Syria Crisis Fair Share Analysis, released on February 1, 2016, Oxfam calculated that only 128,612 resettlement or other humanitarian admission spots had been pledged by the world’s richest governments—still 331,388 below the overall need level of 460,000. UNHCR has reported that some countries have extended other types of visas to Syrians. For instance, Brazil had issued 8,177 humanitarian visas to Syrians affected by the crisis as of February 2016.

The United States, long the global leader in resettlement, admitted only 105 Syrian refugees in fiscal year 2014 through resettlement and only 1,682 in fiscal year 2015. As of January 2016, 645 Syrian refugees had departed so far from Jordan to the United States since October 1, 2015 (the beginning of fiscal year 2016). During calendar year 2016, UNHCR plans to submit roughly 20,000 Syrian refugees to the United States for resettlement consideration, with the substantial majority of these cases coming from Jordan and Turkey. Given lengthy U.S. resettlement processing times, however, the bulk of those Syrian refugees who are ultimately approved for resettlement will most likely not depart for the United States until subsequent U.S. fiscal years.

In Lebanon, the government has taken the position that it cannot be a country of permanent asylum. As a result, UNHCR has concluded that the only durable solution for refugees in Lebanon, other than voluntarily return to their home country (which Syrians cannot do safely now), is to be resettled to a third country.18 However, as of January 2016, only 10,390 have actually departed from Lebanon to resettlement countries—amounting to only 1 percent of the nearly 1.1 million refugees registered in Lebanon. For 2015, UNHCR had only 6,000 resettlement spots pledged for resettlement of refugees in Lebanon. While the numbers have increased recently—with Canada for example resettling 8,200 Syrian refugees from Lebanon between December 2015 and early February 2016, the overall departure level still falls far short of demonstrating a meaningful level of responsibility sharing by the international community.

The United States suspended its resettlement efforts out of Lebanon during 2014 and 2015 due
to the lack of space at the U.S. Embassy for DHS resettlement interviewers. This lack of space for DHS interviewing officers has hampered the U.S.' ability to resettle refugees living in Beirut, including vulnerable refugees with U.S. ties. As discussed in more detail later in this report, resettlement interviews at the embassy are slated to resume during February 2016, but their size and frequency will be limited.

DHS Obtains Extensive Information on, and Rigorously Vets, Syrian Refugees

They are vetted more intensively than any other category of traveler, and this vetting is conducted while they are still overseas. Those seeking resettlement are screened by national and international intelligence agencies; their fingerprints and other biometric data are checked against terrorist and criminal databases; and they are interviewed several times over the course of the vetting process ...

Bipartisan group of former U.S. National Security Advisors, CIA Directors, Secretaries of State, DHS Secretaries, and Retired Military Leaders, December 2015

An extensive array of data is provided to, and obtained by, the U.S. Department of Homeland Security prior to its decision to resettle a Syrian refugee to the United States. This information comes from multiple sources including UNHCR, multiple interviews over a period of years with the refugees, biometric data, documentary materials relating to the specific individuals, and a range of U.S. and international intelligence and law enforcement agencies. Across the region, various data has been collected from Syrian refugees at the time of their registration, as well as during various other interactions with UNHCR and host country governments. Aid workers and resettlement experts repeatedly confirmed that the Syrian refugees resettled to the United States have been living in Jordan, Turkey or other countries for several years already before being referred for consideration for U.S. resettlement.

In Lebanon and Jordan, for example, UNHCR has gathered information from refugees when they are registered, as well as during subsequent interactions. UNHCR has also collected biodata, specifically fingerprints and iris scans, from all registered refugees. UNHCR in Beirut confirmed that, while the Lebanese government has directed it to halt registration of refugees last year, it continues to record information about these refugees, and gathers biodata including iris scans, although these refugees are currently not eligible for third-country resettlement due to their lack of UNHCR registration. In Turkey, the government conducts registration of Syrian refugees and gathers their fingerprints. The Turkish government also identifies cases of vulnerable Syrian refugees to be considered for resettlement. The Turkish government refers these cases—mostly Syrian refugee families facing dire medical issues at this point, though as the Turkish government builds its capacity to conduct these kinds of assessments, other categories of vulnerability are anticipated—to the UNHCR to assess for potential referral to the United States and other resettlement states.

UNHCR Interviews

UNHCR conducts interviews with Syrian refugees before concluding that their cases are appropriate for referral for resettlement. UNHCR refers for resettlement consideration refugees that it considers the most vulnerable. These include survivors of torture and violence, refugees with severe medical needs or disabilities, women at
risk, children at risk, survivors of sexual and gender-based violence, and refugees facing legal and physical protection risks. The overwhelming majority of those resettled are families with children. Only 2 percent of Syrian refugees resettled to the United States are single men, and these men are often survivors of torture or refugees at risk due to their sexual orientation or gender identities.

U.S. Resettlement Support Center Pre-Screening

U.S. Resettlement Support Centers (RSC), funded and contracted by the State Department’s Bureau of Population Refugees and Migration, receive and review the data provided by UNHCR about each refugee’s cases. U.S. resettlement processing officers conduct in-depth interviews that take three to five hours. Human Rights First interviewed one Syrian refugee mother who was interviewed by a U.S. support center officer for five hours, recounting the details of the trauma she and her family suffered in Syria as well as extensive additional information. U.S. resettlement support officers collect biographical information as well as information about the reasons for the refugee’s flight from Syria and other information relevant to eligibility, or ineligibility, for refugee resettlement.

Biographic checks against the State Department’s Consular Lookout and Support System (CLASS)—which includes watch-list information—are initiated at the time of prescreening by the State Department’s Resettlement Support Center staff. CLASS contains information from a variety of intelligence and law enforcement sources, including TECS (formerly the Treasury Enforcement Communication System), the Terrorist Screening Database (TSDB), the Drug Enforcement Agency (DEA), the Federal Bureau of Investigation (FBI) and Interpol. As outlined below, Interpol has extensive intelligence and law enforcement databases, which include information from 50 countries as well as specific databases relating to suspected terrorists, foreign fighters and stolen, lost and blank passports. Following this initial pre-screening, the United States continuously vets applicants throughout the application process, up to and even beyond their arrival for resettlement.  

Documentary Materials Gathered and Vetted

The United States government gathers extensive documentation from Syrian refugees during this process, including birth certificates, school certificates and passports. In fact, Syrian refugees are more highly documented than other refugee populations according to U.S. resettlement workers. As confirmed in a recent Congressional hearing, DHS has the ability to test for false passports through a well-developed component of its screening process. Interpol has an extensive database of information relating to lost, stolen, and “blank” passports from 170 countries—including from both Syria and Iraq.  

Pre-Vetting—Enhanced Review of Syrian Cases

Each Syrian refugee case is pre-vetted in Washington D.C. by DHS-USCIS headquarters, before a DHS-USCIS officer conducts an interview with the refugee. All cases that meet certain criteria are referred to the DHS Fraud Detection and National Security Directorate for additional review and research, including open-source and classified national security research. According to DHS, the pre-vetting generates case-specific context and information to inform lines of questioning used by DHS-USCIS officers during refugee interviews. DHS has reported that this directorate engages with law enforcement and intelligence community members for assistance with identity verification as well as the acquisition of additional information.
DHS Refugee Interviews
Trained DHS-USCIS refugee corps officers travel to U.S. resettlement locations—such as Amman and Istanbul—to conduct extensive refugee interviews with each refugee. Refugee officers receive specialized training that includes comprehensive instruction on fraud detection and prevention, security protocols, interviewing techniques, credibility analysis and current conditions in the country at issue. Before deploying overseas, officers receive pre-departure training which focuses on the specific population they will interview. This includes detailed updates on any security issues or fraud trends. USCIS officers adjudicating Syrian claims also receive an additional one-week training on country-specific issues that includes briefings from experts from the intelligence community. Upon deployment, these officers conduct detailed inquiries to gather information relating to the individual’s credibility, the persecution the refugee has faced, and whether any activities or actions of the refugee would make him or her inadmissible to the United States on security, criminal, terrorism or other grounds. During an interview lasting three, four, and sometimes five hours, the officer assesses the credibility of the applicant and evaluates whether the applicant’s testimony is consistent with known country conditions. All refugee status determinations made by interviewing officers undergo supervisory review before a final decision is made. According to DHS, certain categories of cases—including certain national security-related cases—must in addition be submitted for further review by DHS-USCIS headquarters in Washington prior to the issuance of a decision. There, headquarters staff may liaise with law enforcement and intelligence agencies and consult with outside experts before finalizing the decision.23

Security Clearance Process
The Department of Homeland Security conducts and coordinates extensive vetting, including with domestic and international intelligence and law enforcement agencies. These include checks conducted by the National Counterterrorism Center, FBI Terrorist Screening Center, Department of Defense Biometric Screening and the State Department’s Consular Lookout and Support System. The clearance process checks against watch list information as well as broader domestic and international intelligence community holdings from Interpol. (Jordan, Turkey, Egypt and Lebanon are all Interpol members.) Interpol’s Foreign Terrorist Fighter database—which is supported by a working group that includes Turkey and the United States—includes detailed identity particulars and profiles of individuals travelling to or from Syria and Iraq, comprised of information provided by more than 50 countries. Interpol’s Stolen and Lost Travel Documents (SLTD) database includes details of nearly 54 million stolen, lost, blank, and other documents from 170 countries—including from Syria and Iraq.24 As of September 2015, Interpol’s database of suspected terrorists included more than 10,000 names. The U.S. National Central Bureau (NCB) for Interpol is run by DHS and DOJ, which manage U.S. access to the organization’s extensive criminal and terrorism databases, as well as its lost and stolen passport database.25 In addition to Interpol, the United States maintains direct intelligence relationships with countries like Jordan, where refugees have been living for years. For example, the United States and Jordan have been reported to be collaborating in countering extremism through “Operation Inherent Resolve,” which includes intelligence sharing. Much of the information the United States government receives from foreign partners is classified.26
Understaffing and Backlogs Continue to Hamper the Already Slow U.S. Resettlement Process

The United States committed to resettle 85,000 refugees from around the world during fiscal year 2016, including "at least" 10,000 Syrian refugees. As of January 31, four full months in to the fiscal year, the United States has resettled only 841 Syrian refugees during the 2016 fiscal year, which will end on September 30, 2016.

Across the region, it is clear that U.S. resettlement processing centers and U.S. agencies (including the State Department’s PRM and DHS-USCIS) are working hard to try to meet the U.S. commitment to resettle Syrian refugees, and the number of DHS officers traveling to the region to interview Syrian refugees has increased. The U.S. Resettlement Support Centers (the International Catholic Migration Commission and the International Organization for Migration, organizations with extensive experience) have scaled up their processing and are devising strategies for addressing the logistical challenges associated with larger DHS interview visits.

UNHCR is also working hard to refer cases to the U.S. resettlement program, as well as to other countries with less slow resettlement or admissions processes. As of mid-January 2016, DHS-USCIS reported that the U.S. resettlement program had received about 26,500 referrals of Syrian refugee applicants for consideration, mostly from Jordan and Turkey as well as some from Egypt. In Jordan, it is anticipated that UNHCR will submit 11,000 Syrian refugees for U.S. resettlement consideration in calendar year 2016. In Turkey, UNHCR will refer over 8,000 Syrian refugees for U.S. consideration in 2016, as well as another 1,000 from Lebanon. Of course, given U.S. processing times, the bulk of these cases are not likely to be actually resettled to the United States until subsequent years, and not all will ultimately be approved for U.S. resettlement.

Despite these significant efforts, a number of factors—primarily relating to understaffing—are unnecessarily delaying parts of the process, which, even without lengthy delays, typically takes 18 to 24 months to complete. The factors hampering resettlement, which are outlined below, include the backlogs in review of "hold" cases, the need for additional security vetting staff to timely conduct inquiries on both resettlement and SIV cases and the lack of space for resettlement interviewers at the U.S. Embassy in Beirut. In addition to impacting Syrian resettlement and the processing of SIV applicants who worked with the U.S. military in Iraq and Afghanistan, these backlogs also delay resettlement processing for Iraqis who have priority access to resettlement due to their work with the U.S. military, contractors and other U.S. entities. There is already a tremendous backlog of over 50,000 Iraqi resettlement cases, including Iraqis who worked with the U.S. military. Many have been waiting years already, often stranded in dangerous or difficult situations.

Backlogs in Review of Hold Cases

After DHS officers conduct their lengthy interviews with Syrian refugees, a majority of these cases go into a limbo where they remain stuck in a backlog, with no decision made, often for extended periods of time, waiting their turn for time from a DHS officer to conduct additional review of the case. About 4,000 to 5,000 Syrian refugees were estimated to be in this "no decision" limbo as of January 2016. Cases may be referred into this hold category for various reasons, including to sort through legal or factual issues relating to issues such as detention by the Syrian government. In addition, many peaceful pro-
democracy advocates have been jailed and tortured by the regime, and never engaged in activity aimed at supporting ISIL or other terrorist groups, yet their cases can be delayed for many months or longer as they wait in the backlog. Some resettlement cases may raise potential issues of inadmissibility under DHS’s interpretation of the immigration laws, when, for instance, ISIL or another armed group in command of areas within Syria has demanded that innocent civilians pay them “taxes” or other fees. Many of these cases involve broad factual scenarios that affect large numbers of innocent and vulnerable Syrians who have faced persecution in Syria and actually do not present any risk whatsoever. These cases are swept into this review as part of a purposefully overly broad sweep; as a result many will ultimately be resolved positively as they do not actually present any risk.

If additional DHS staff were dedicated to reviewing these cases in a prompt (and thorough) manner, the backlogs could be eliminated or significantly reduced. Careful assessment might also reveal whether categories of individuals who present no threat are unnecessarily added into this backlog. Effectively addressing this backlog would also assist in meeting U.S. resettlement goals and improving the efficiency of the process. Additional DHS-uscis resources and increased oversight would help to address some of the delays in resolving holds under the Controlled Application Review and Resolution Program (“CARRP”), a program which is discussed below.

As a result of the backlogs of cases waiting for review by DHS officers, the departure of refugees to the United States are now below anticipated goals. The impact of unnecessary delays on refugees awaiting resettlement—as well as on the effectiveness and reputation of the U.S. resettlement system—is devastating. A recent New York Times magazine article noted that, “among Syrian refugees, ‘on hold’ is the most dreaded category, and that it is extremely difficult to get clear answers about why a hold has been applied or when it will be lifted.”27 The article recounted the story of a Syrian refugee couple whose application for U.S. resettlement became stuck on hold. The father said that if the family did not get a call from the U.S. resettlement program by the spring 2016, they would leave for Europe—even though they had family that they desperately wanted to join in the United States. While he and his wife did not want to take their two toddlers on this dangerous trip, they were unable to support themselves any longer and felt that they would have no choice. Human Rights First interviewed a Syrian family in Turkey who are facing an identical dilemma for the same reasons.

Resettlement and SIV Delays Due to Lack of Adequate Staffing for Timely Security Vetting

While some steps in the U.S. security vetting process can take some time to complete, the security vetting process is also impacted by delays that are caused by lack of sufficient staffing to conduct inquiries and follow up relating to security vetting. For instance, if a refugee has a name similar to that of a known terrorist, careful follow up review would need to be conducted. A review of data would often make clear that the refugee was a not in fact that individual. But intelligence and other security vetting agencies often lack enough staff, or do not allocate enough staff, to conduct prompt security vetting follow-up for both refugee and Special Immigrant Visa applicants.

However, if DHS and the relevant security vetting agencies hire or allocate additional staff, with strong expertise and training on the Middle East, and are directed to make completion of these cases a priority, this processing can move ahead in a more timely manner. As pointed out by former Ambassador Ryan Crocker—who contended with the backlogs delaying resettlement of Iraqis...
whose lives were at risk because of their work with the United States when he served as ambassador to Iraq under President George W. Bush—President Obama can address these backlogs "without weakening security by simply directing security agencies to devote more time and staff to the task." It is certainly not in the security interests of the United States to have delays in security vetting, which would potentially delay identification of any individuals who might present a security threat to the United States or its allies in the region. Moreover, as numerous national security experts have confirmed, an effective resettlement initiative actually advances U.S. national security interests by supporting the stability of the region around Syria and U.S. allies.

DHS also needs additional staff resources and oversight support to address backlogged cases that have been put on Controlled Application Review and Resolution Program ("CARRP") hold and are waiting their turn for review and resolution. The U.S. government is using the secret CARRP process on resettlement cases, including Syrian refugee cases, as described in a recent media article. According to a DHS- USCIS memorandum cited in that piece, if any potential national security issue is raised during the vetting process, including from security checks, the case is referred for "a focused national security CARRP review." In a 2013 report on the CARRP program and its impact on applicants for U.S. citizenship and status, the ACLU wrote that the CARRP categories "cast extremely wide nets, rely on discriminatory profiling, and yield imprecise, inaccurate and often absurd results that disproportionately impact [Arab, Middle Eastern, Muslim, and South Asian] applicants." For Syrian refugees, the broad CARRP categories are believed to cover many who do not actually present security threats—including, for example, pro-democracy advocates arrested by the regime and civilians forced to pay "taxes" to armed groups. Given the need to identify any real security threats, and the importance of moving ahead on cases where there is no threat, additional DHS staffing, resources, and oversight could help address some of this backlog.

Lack of Accommodation for DHS Refugee Interviewers at U.S. Embassy in Lebanon

While the United States is restarting resettlement in Lebanon in February 2016, that resettlement effort will be minimal. For calendar year 2016 (which includes a portion of the 2017 U.S. fiscal year), the United States will take only about 2,500 refugee referrals for consideration in Lebanon. These numbers fall far short of the kind of U.S. leadership that can help encourage other states to increase their resettlement initiatives, and in turn, support the fragile stability of tiny Lebanon which is struggling under the weight of hosting over one million Syrian refugees, amounting to one out of every four people in the country now.

The United States had suspended its resettlement efforts out of Lebanon during 2014 and 2015, as noted above. In December 2015, a U.S. Embassy public affairs officer stated that "[d]ue to resource and space constraints, the United States has not been able to conduct refugee admission interviews at U.S. Embassy Beirut since August 2014." DHS requires its officers who travel to Beirut to live and stay in the U.S. Embassy compound. The lack of space made available for U.S. resettlement interviewers has greatly hampered U.S. ability to resettle refugees living in Beirut. In Lebanon, Human Rights First met an Iraqi refugee who had worked for the U.S. government in Iraq for over 5 years. Yet he and his family have been struggling to survive in Lebanon for years, and he was told that there was no resettlement to the United States from Lebanon.
U.S. resettlement interviews are slated to begin again in February 2016. However, the number of resettlement interviews will be limited, with only four fairly short “circuit rides” visiting in the remainder of this fiscal year, one in February, one in May, one in July, and another in September. The circuit rides are anticipated to include only about 4 interviewing officers due to the Embassy’s lack of space for the officers. All in all, U.S. officers will likely handle a little over 200 cases on each visit, interviewing 500 people (as each case may include multiple family members), for a total of about 2,000 refugee interviews. Not all will be accepted to the United States, and some will be put on hold—added to the substantial backlog of no decision cases on hold while they wait for review after their DHS interviews.

Most of UNHCR’s recent resettlement referrals to the United States in Lebanon have been of Iraqi refugees, as other resettlement countries are requesting Syrians and some very vulnerable Iraqi refugees are also in need of resettlement. As of January 2016, only 83 of the resettlement submissions made to the United States by UNHCR in Lebanon since October 2015 were for Syrian refugees and only 25 Syrian refugees had actually been resettled from Lebanon to the United States since October 2015.

The U.S. Embassy in Beirut is moving ahead to secure additional space, and this overdue effort should be a top priority for the Embassy so that the expansion moves ahead without further delay. In the meantime, more effort should be focused on interim steps to increase space for DHS resettlement officers within the Embassy compound. UNHCR will also need additional resettlement staffing to increase its referrals to the United States for resettlement consideration.

Capacity Gap in DHS Refugee Corp Staffing and Circuit Rides

DHS refugee corps officers travel to Jordan, Turkey, Lebanon, and other resettlement processing locations to conduct interviews, in what are called “circuit rides” to the region. While DHS is making an effort to increase the size of its refugee officer circuit rides to the region, there are still gaps between visits in some locations that can leave refugees waiting for months or longer for a DHS interview. In Turkey, circuit rides are now nearly continuous. DHS should increase the number of refugee officers for each circuit ride on a longer term steady basis in order to provide more continuous coverage, particularly in locations where there are longer periods of time between circuit rides. DHS must also address the staffing level deficiencies and attrition challenges that face both the USCIS refugee corps and the Asylum Division. Given that the world is facing the largest refugee crisis since World War II, DHS and USCIS should take steps to increase the size of the refugee corps. Redeploying trained DHS-USCIS asylum officers to conduct overseas resettlement interviews will add to the already growing backlogs in the affirmative asylum process, backlogs that have grown due in part to the decision to subject Central American families to the expedited removal process. 31

Gaps in Capacity for Resettlement Referrals

In order for the United States to step up its resettlement of Syrian and other refugees, it needs to have cases referred to it for consideration by UNHCR and other trusted sources. UNHCR staff have been working hard to identify and refer cases for resettlement consideration to the United States and other countries. Yet, with many humanitarian appeals underfunded, UNHCR has been faced with significant funding short-falls, leading to cuts in staffing across the agency, including in areas related to resettlement referrals. UNHCR also has
to identify cases for referral to other countries, with resettlement and other programs that will move people more quickly. Moreover, while the United States will need more referrals from UNHCR to meet its targets, the backlogs, delays, and the low departure numbers for U.S. processing may, if not remedied, ultimately discourage referrals to the United States, particularly as other countries’ resettlement and humanitarian admissions efforts move ahead in a more timely manner.

The United States and other countries should step up contributions to UNHCR to increase its capacity to identify, assess, and refer cases for U.S. and other resettlement and humanitarian admission programs. The United States should also allow trained U.S. based non-governmental organizations, with expertise in U.S. resettlement processing and operational capacity in the region, to refer vulnerable refugees in need of resettlement directly to the U.S. resettlement program for consideration and assessment. In addition, UNHCR field offices should work with trained and trusted non-governmental organizations that can help identify, gather information on, and refer cases to UNHCR for its refugee status and resettlement assessment. This strategy would increase UNHCR’s capacity by freeing up its time to focus on the more substantive aspects of the refugee and resettlement assessment.

The U.S. State Department just, as of February 2016, instituted a priority processing category for Syrian refugees with U.S. family ties. The creation of a priority (P2) category for Syrian refugees with approved family visa (I-130) petitions allows these cases to apply directly to U.S. resettlement processing support centers. These resettlement candidates will still be fully vetted by U.S. support centers, by USCIS-DHS officer interviews, and by the various U.S. and international security vetting agencies. They would simply skip the step of a

UNHCR referral in light of their family ties in the United States and the prior approval by DHS-USCIS of their U.S. family petition.

About 4,000 Syrians, with U.S. family and approved I-130 petitions, are currently living as refugees in the region. Many Syrians with approved I-130s are currently located in Syria, but as the countries surrounding Syria have largely closed their borders, Syrians with U.S. family would generally be unable to leave Syria in order to cross to another country as refugees to seek processing of their cases. The United States could—and should—negotiate permission for some of these Syrians to cross the border as needed for purposes of U.S. processing in those neighboring countries where the United States conducts processing. In addition, the United States should expand priority access to Syrian refugees (and their respective spouse and children) with relatives (at least spouses, children whether over or under 21 and whether married or unmarried, parents and siblings) in the United States who have any kind of lawful immigration status in the United States or have an application for such status pending.

Lack of Sufficient Capacity to Expedite Processing for Refugees Facing Imminent Risks

Across the region, Human Rights First has spoken with, and heard additional reports of, Syrian refugees who face imminent risks of harm and were in need of immediate protection and expedited resettlement processing. In some cases, these refugees faced risks of physical harm due to their sexual orientation or gender identity. In other cases, refugees who had been engaged in peaceful political, human rights or humanitarian activities in Syria were threatened or targeted—in Turkey or in Lebanon—by individuals associated with militant or terrorist groups. Human Rights First was in contact with a young refugee in Lebanon, a survivor of torture in Syria, who was
shot at by Hezbollah supporters in Lebanon. Unable to find protection in Lebanon in this emergency, after receiving further threats from the same source he fled the country for Europe where he is now seeking asylum. The dangers facing individual refugees in Turkey who are perceived to be threats to ISIL have been documented in the press. For instance, in December 2015, a Syrian journalist, who had worked with a prominent anti-ISIL group was shot in Gaziantep, Turkey. He was slated to have left Turkey for France just that week on an asylum visa. In October 2015, two anti-ISIL activists were found beheaded in the southern city of Sanliurfa, in murders claimed by ISIL. All were members of Raqqa is Being Slaughtered Silently, a group dedicated to documenting ISIL’s human rights abuses, as well as violations by the Syrian government and rebel groups. Human Rights First spoke to another refugee in Turkey who is similarly situated, at urgent risk, and was not receiving assistance with protection in Turkey or resettlement outside it. UNHCR lacks sufficient staff, resources and strategies to provide refugees facing security risks with meaningful short term protection.

The United States has improved its capacity, in at least a small number of cases, to resettle at-risk refugees in a more timely manner, but this capacity is very limited and the “expedited” cases still do not move quickly as do the processes of a few other countries. As a result, UNHCR sends cases involving imminent risks to other countries that have real expedited processing capacity. While other countries do have these programs, it makes little sense to resettle a refugee with strong ties to—or in—the United States to a Scandinavian or European country.

No Shows and Pull outs

An additional factor that could hamper U.S. resettlement of Syrians is the decision of some families—who have already been struggling to survive for years in Turkey and other countries in the region—to pull out of the prolonged U.S. resettlement process, in some cases because they have given up hope while waiting and decided to take the dangerous trip to Europe. Aid workers and resettlement experts in the region report that some Syrian refugees who have been referred to the United States for resettlement consideration have pulled out of the process or taken steps that result in their cases being pulled out of the process. The U.S. process takes nearly two years and often much longer to complete. In some cases, refugees—who were already living in exile in Turkey or elsewhere for years—have lost hope in the process. In Turkey, an estimated 20 to 30 percent of cases in the U.S. resettlement pipeline have pulled out of the process or not shown up for interviews. While there are some similar reports in Jordan and Egypt, the numbers are much lower. As detailed earlier in this report, Syrian refugees are increasingly unable to survive in front-line refugee-hosting states. In other cases, one or more members of a family that was waiting for resettlement consideration have decided to risk the dangerous trip to Europe as they believe their family can’t survive for another year or two. The complete lack of certainty as to how long the process may take in any particular case in the U.S. resettlement system, and the specter of disappearing into an adjudication delay of indefinite duration even after the interview, contribute to refugees’ despairing of the process. Resettlement support staff are adopting proactive strategies for keeping refugees more closely informed about the progress of their resettlement cases and to minimize the potential for a DHS interview slot to be wasted.

Continuing Backlogs in Resettlement of U.S. Affiliated Iraqis

Iraqi refugees and many Iraqis who worked with the United States military or other U.S. entities are also stranded in the region. Processing backlogs and challenges have also delayed the
resettlement of Iraqis including those who have direct access to U.S. resettlement consideration because they worked with the U.S. military, contractors, non-governmental organizations, and media, as well as Iraqi refugees with U.S. families. Over 50,000 Iraqis, many of whom have U.S. ties or have worked for the U.S. military and government, are waiting in a U.S. resettlement backlog. Many been waiting years to be brought to safety in the United States. The processing of these cases has been delayed by a number of backlogs, including the backlog of cases waiting for follow-up review by DHS or other security vetting staff. The American SAFE act, which passed the House of Representatives in December, would have, if enacted, further delayed the resettlement of these and other Iraqi refugees, as well as Syrian refugees.

deficit grew to $2.6 billion USD. The Syrian conflict cost Lebanon an estimated $7.5 billion USD in cumulative economic losses between 2012 and 2014—including additional costs incurred for borrowing to support increasing demand for public services. It has been estimated that unemployment among Lebanese increased from 8.1 percent in 2010 to 13 percent in 2013-2014, pushing an additional 170,000 people into poverty. UNHCR reports that the added pressure on infrastructure brought on by the number of refugees in Lebanon has "severely affected water and sanitation systems" throughout the country. Refugee families have reported walking miles to obtain clean drinking water, and using sewage water to clean, shower, and wash dishes and clothes. The infrastructures of Jordan—including water, electricity, sanitation, health care, and education—have also been heavily impacted by the number of Syrian refugees the country is hosting. The Carnegie Endowment for International Peace has written that "even before the influx of Syrian refugees, Jordan’s population was expected to double by 2024, while the water supply was projected to decrease by half. The arrival of hundreds of thousands of Syrian refugees doubled demand for water in some parts of the country, with communities hosting the largest numbers of refugees experiencing the heaviest burdens. In some northern parts of Jordan, where many Syrian refugees reside, average daily water supplies now stand at below 30 liters per person, though 80 liters are required to satisfy a family’s minimum needs. Solid waste management has also become more difficult, as Syrian refugees add an estimated 340 daily tons of waste to Jordan’s waste volume. Warning his country was at a “boiling point,” King Abdullah II of Jordan stated that the number of Syrian refugees “hurts us when it comes to the educational system, our healthcare.” The number of Syrians

Impact on Front-Line Refugee Hosting States and U.S. National Security Interests

How can we be a contributor to regional stability if we are let down by the international community?

King Abdullah II of Jordan

The large numbers of Syrian refugees now living in Lebanon, Jordan, and Turkey have placed tremendous strains on those countries and their critical infrastructures. UNHCR has concluded that Lebanon, which hosts more than 1.19 million Syrian refugees, has "the highest per capita proportion of refugees to population in the world," placing "enormous pressure on the country and its people" and stretching the country’s infrastructure and economy. Between 2012 and 2014, the Lebanese economy contracted and the national
in need of medical assistance had strained the country’s health care system, leading to shortages in hospital beds in Amman and prompting some Jordanians to seek care through private health providers. The Jordanian education system has also been affected by the addition of Syrian children, leading to shortened class times, overcrowded classrooms, and double-shifting, in which schools operate in two shifts that serve different groups of students at different times in the day.  

In Turkey, the number of refugees is also impacting some of the country’s critical infrastructure—particularly in areas hosting higher proportions of Syrian refugees. In a December 2015 report, the World Bank Group stated that the addition of thousands of Syrian refugee children to Turkey's education system has prompted a 40 to 60 percent increase in enrollment, straining the country's schools and forcing Turkey to open temporary education centers to address the enrollment crisis. Housing markets have also suffered: though no market assessment currently exists, figures commonly cited in Turkey report that housing prices have nearly doubled in some areas, particularly along the Syrian border, and that the refugee crisis has led to decreased housing availability. Although Turkish facilities have expanded drastically to accommodate increased demand for healthcare among Syrian refugees, some Turks have nonetheless described long waits and overcrowding at health centers. The Migration Policy Institute concluded in a mid-2015 report that “by early 2015, the cost [of the Turkish government providing camp-based services and economic assistance to urban Syrian refugees] had reached more than $5 billion USD, of which the international community covered some 3 percent.”

These countries have repeatedly asked for support from the international community, including through humanitarian and development assistance, bilateral aid, and help from other countries to share in hosting some portion of Syrian refugees. In May 2015, President Erdogan of Turkey, urged other countries to do their “duty” to accept more Syrian and Iraqi refugees, noting that Turkey had spent large sums to host and care for Syrian and Iraqi nationals. In October 2015, Lebanese Finance Ministry Director-General Alain Bifani asked for interest-free international aid to assist Lebanon in combatting the Syrian refugee crisis. Stressing that the world should consider accepting refugees as a “global public good,” he noted that public infrastructure and hosting communities have been stretched “to the limit” under the tremendous burden of millions of Syrian refugees. In January 2016, Jordanian government spokesman Mohammed Momani offered to fly some 17,000 refugees amassed on the Syrian-Jordanian border to any country willing to accept them.

Representing an important step forward in terms of assistance, the February 4, 2016 donor conference in London led to over $10 billion USD in pledges. These included significant pledges of development assistance and a move towards strategies that could provide employment and other opportunities for both Syrian refugees and host communities. However, as discussed above, despite some progress on pledges to actually resettle or admit Syrian refugees, the international community is still falling far short of meeting that need.

Experts on the region have explained that a significant Syrian refugee resettlement initiative would help support the stability of these front line refugee hosting states. As Ryan Crocker, former U.S. Ambassador to Afghanistan, Iraq, Pakistan, Syria, Kuwait, and Lebanon, has explained:

A U.S. initiative to resettle Syrian refugees in the United States affirmatively advances U.S. national security interests. Increased resettlement and aid helps protect the stability
of a region that is home to U.S. allies, including Jordan, Lebanon, and NATO member Turkey, all of which are hosting large numbers of refugees. The infrastructure—water, sewage, medical care, and education—of these states is overwhelmed. A major resettlement and aid initiative can relieve that strain. But left unaddressed, the strain will feed instability and trigger more violence across the region, which will have negative consequences for U.S. national security.

A bipartisan group of former high level U.S. national security leaders—including former Secretaries of Homeland Security Michael Chertoff and Janet Napolitano, former National Security Advisor Stephen Hadley, former CIA Directors General Michael Hayden, U.S. Air Force (Ret.) and General David Petraeus, U.S. Army (Ret.), and former Secretaries of State Madeleine Albright and Henry Kissinger—has also confirmed the importance of resettlement in advancing U.S. national security. They explained that “resettlement initiatives help advance U.S. national security interests by supporting the stability of our allies and partners that are struggling to host large numbers of refugees,” and also pointed out—in response to proposals that would have halted Syrian resettlement—that “[c]ategorically refusing to take them only feeds the narrative of ISIS that there is a war between Islam and the West, that Muslims are not welcome in the United States and Europe, and that the ISIS caliphate is their true home.” Michael Chertoff, DHS Secretary under the administration of George W. Bush, told the Wall Street Journal that “You don’t want to play into the narrative of the bad guy. That’s giving propaganda to the enemy.”

Factors Contributing to Push Refugees to Europe

In addition to serving as a concrete expression of responsibility sharing, humanitarian or additional pathways for admission can reduce the need for refugees to resort to irregular and dangerous onward movements.

UNHCR Background Note for March 30, 2016 Meeting on Responsibility Sharing

Many refugees will choose to seek protection in locations where they have family. As one resettlement aid worker noted, “overwhelmingly refugees want to go where they have family.” Aid workers across the region told Human Rights First researchers that, in their experience, many Syrian refugees had some family living in Europe, a comment borne out by the accounts of refugees we interviewed. These included a mother who intended to leave Turkey to join her sons in Germany and a Syrian woman in Jordan whose brothers were all refugees in Sweden. Some, though fewer, have family in the United States. When refugees live near family, both they and States hosting refugees benefit from that added layer of support.

Human Rights First’s research confirmed that the many serious protection deficiencies outlined in this report are also contributing to the movement towards Europe. Indeed, the lack of effective regional protection, exacerbated by the lack of sufficient assistance and orderly resettlement or visa routes for refugees, is driving many Syrians to embark on dangerous trips to Europe in search of protection. As noted above, roughly half of refugees in Jordan were thinking of taking the dangerous trip to Europe given their lack of permission to work and lack of sufficient

HUMAN RIGHTS FIRST

627
assistance, according to a CARE International survey.

As aid workers in Jordan told Human Rights First researchers, over the second half of 2015, more Syrian refugees began indicating that they wanted to leave the country. After years in exile, these refugees indicated that they didn’t see a future for their children. They have lost hope that the conflict will end. Their savings are depleted. They don’t have the resources to pay the fees and transportation costs to send their children to school. They do not want to be dependent on assistance, and in any event, the limited amounts of assistance have been sharply cut so do not cover even basic needs. They cannot work legally and they cannot survive under these circumstances. As some refugees who went to Europe told aid workers, they “had nothing to lose” and were “dying every day” in Jordan.

As UNHCR has noted, the second half of 2015 saw an increase in the movement of Syrian refugees both through and from Lebanon to Europe. Over 150,000 refugees reportedly transited to Europe through or from Lebanon, with the vast majority transiting only briefly through Lebanon. Indeed, given the prohibitions on entry and registration implemented in Lebanon in January and May 2015, Syrians fleeing their country would generally not be authorized to stay in Lebanon by the authorities. With respect to Lebanon, UNHCR has concluded that “[t]he deteriorating protection environment (such as inability to renew residency) and dwindling assistance for Syrians in Lebanon, coupled with a lack of livelihood opportunities, have led more Syrians in Lebanon to express their intention to move onward to third countries.” In Turkey, as one aid worker told Human Rights First researchers, many Syrian refugees have said that they would stay if they had a job and education for their children. Multiple Syrian refugees expressed to us these same two priorities, emphasizing that what they needed was education for their children and work that would allow them to provide a dignified life for their families.

In Turkey, but also in Jordan, Egypt and Lebanon, Human Rights First researchers heard reports that refugees who had already been struggling to survive for years in the region lost hope in waiting years longer for the limited potential of resettlement and instead embarked on the journey to Europe. Aid workers told Human Rights First that some refugees awaiting resettlement decided that they can’t wait longer and instead made their way to Europe. As one aid worker in Lebanon said, in some cases the refugees “lost hope in the resettlement process” because it is so lengthy. One resettlement expert living in Lebanon told us about a young Syrian woman, who had family living in Europe, but after waiting for years for a potential resettlement opportunity to move ahead, she finally gave up waiting and took the dangerous trip to Europe to join family who could help her.

The delays in U.S. resettlement, along with the other factors outlined in this report, have also contributed to the decision of some refugees, who have already waited years for a route to resettlement, to abandon their waits and try to reach Europe. As outlined above, some refugees who are waiting for U.S. resettlement—including refugees who are already in the U.S. processing “pipeline”—have pulled out of the process or given up waiting, in some cases traveling on to Europe. Human Rights First received reports of these "no shows" or pull outs in connection with U.S. resettlement processing in Turkey primarily, but also in Jordan and Egypt. As one aid worker in Jordan explained, the U.S. resettlement process is "very, very long." U.S. resettlement processing officers are however working to increase their communication with refugees during the lengthy processing wait times in an effort to reduce the potential that refugees.
Questions Concerning Christian Refugees

Some U.S. politicians have asked whether Christian refugees from Syria are being blocked from resettlement. Human Rights First researchers found no indication of any efforts to limit resettlement of Christian refugees from Syria. UNHCR staff and statistics repeatedly confirmed that resettlement rates for Christians are in line with the overall registered refugee population. Aid workers across the region confirmed that a slightly higher portion of Christian Syrians are believed to have fled to Lebanon, rather than to Turkey or Jordan, given Lebanon’s geographic proximity to several important areas of Christian settlement within Syria and the existence of a significant Christian community in Lebanon. As detailed in this report, the United States has conducted only very limited resettlement in Lebanon, suspended resettlement from there for about a year, and has resettled only a handful of Syrian refugees from Lebanon so far.

Given long resettlement processing times and multiple hurdles, Syrian refugees, including any Syrian Christians, are often stuck in the backlog of Syrian cases. One media story profiled the multi-year resettlement wait experienced by an Armenian Christian family that fled Syria in 2012. Many refugees, including Christians, may moreover find their resettlement cases delayed or denied due to ISIL demands that individuals pay “taxes” to ISIL. Payments to armed groups have been interpreted as “material support” to terrorist organizations under sweeping inadmissibility provisions of U.S. immigration law. While inadmissibility waivers can be granted in some cases, the entire waiver process has been plagued with delays for years.

Moreover, the U.S. has resettled a high proportion of Christian refugees from Iraq. These refugees, many of whom were referred to the United States for resettlement consideration by UNHCR, given the circumstances of their individual cases, fell within the parameters of broader resettlement initiatives that prioritized resettlement of vulnerable refugees as well as, through a U.S. initiative, Iraqis with U.S. ties.

As recommended in this report, the United States should expand resettlement out of Lebanon and prioritize efforts to assure that space at the U.S. Embassy in Beirut is allocated to resettlement. Various resettlement experts working in the region surrounding Syria confirmed that if the United States were to institute a special resettlement path for Christian refugees that host countries would likely block these efforts. The United States should however, as it did with Iraqi refugees, continue to prioritize resettlement of vulnerable Syrian refugees. The U.S. Commission on International Religious Freedom reiterated its support for continued resettlement of Syrian refugees in December 2015 and called on the United States to prioritize the resettlement of Syrian refugees based on their vulnerability.
In Turkey, for instance, Human Rights First researchers learned that in some cases families who had been waiting for resettlement to the United States had “lost hope.” Human Rights First spoke with a Syrian woman who had already been interviewed for resettlement to the United States and received a no decision letter. She was contemplating taking to the sea along with her children because she cannot survive any longer in Turkey. Resettlement workers learned in some cases that Syrian refugee fathers, unable to feed and support their families in Turkey, decided to try to reach Europe to find a more immediate solution to the need to feed and support their families. In addition, media and social media reports about the opposition by some U.S. politicians to Syrian resettlement—and proposals to ban Muslims—have reverberated across the region and left some Syrian refugees fearful of resettling to the United States or afraid that U.S. resettlement will be terminated. After hearing about renewed efforts in Washington in January 2016 to block resettlement of Syrians, one Syrian woman who was awaiting U.S. resettlement, explained that she and her husband feared the United States was shutting its borders to Syrian refugees and “[a]fter all the news, we have no hope to travel to America.”

Resettlement of Women, LGBT, and other Vulnerable Refugee Populations

The populations referred for U.S. resettlement consideration include very vulnerable refugees, such as torture survivors, families headed by women, LGBT persons, and families facing grave medical threats. Due to the lack of adequate medical care for refugees and the steep cuts in medical care, refugees who face dire medical threats have been in particular need of resettlement. As noted above, aid workers involved in the resettlement process repeatedly confirmed to Human Rights First researchers that they were working to refer vulnerable refugees for resettlement consideration by U.S. authorities.

In some countries, Syrian and other refugees face imminent risks of violence or harm, even though they are no longer in their home countries. For example, some Syrian refugees who engaged in peaceful humanitarian or political activity in Syria have been attacked in Lebanon by armed actors supportive of the Assad regime. LGBT refugees face a range of risks in the region, including difficulties accessing UNHCR due to negative attitudes of local staff toward LGBT persons. LGBT refugees can also face violence, detention and torture in detention, including in Lebanon, Jordan and Turkey. In the region, Human Rights First researchers were told that UNHCR often does not refer LGBT cases to the United States for resettlement because the U.S. resettlement process takes too long and would leave these refugees at risk of harm for too long while they wait.
Recommendations for U.S. Leadership of a Global Initiative

History has demonstrated that earlier [refugee] efforts strengthened not only the fabric of our society, but also our leadership role in the world.

Former National Security, International Humanitarian and Human Rights Appointees of both Democratic and Republican Administrations, September 2015

While efforts to resolve the Syria conflict continued in early 2016, peace and the potential for safety, security, and rights-respecting conditions in Syria continue to be as elusive as ever. Given the overriding humanitarian, human rights, foreign policy, and national security interests at stake, the United States should lead, working closely with European allies and other countries, a comprehensive response to the Syrian refugee crisis and the broader global displacement crisis. Both the president and Congress will have multiple opportunities to demonstrate strong U.S. leadership over the coming months. These opportunities include: a March 30 Syrian resettlement pledging conference in Geneva, the World Humanitarian Summit in May, the setting of fiscal year 2017 goals for U.S. resettlement, appropriations and budgeting for fiscal year 2017, and the U.S. and U.N. conferences on the global refugee crisis, and large movements of refugees and migrants respectively, both slated for September 2016 in New York. This leadership will require high-level engagement from the president, the secretary of state, and secretary of Homeland Security, and the support of Congress.

In order to effectively lead, to press other states to do more, and to advance U.S. national security and foreign policy interests, the United States must significantly increase its own humanitarian assistance, development investment, and resettlement commitments. U.S. political leaders should work together in a bipartisan manner, restoring this country’s long bipartisan tradition of protecting those who flee persecution. The United States has demonstrated strong leadership in the past—launching a comprehensive global effort with other countries to help Vietnamese refugees—and is more than capable of leading by example again.

To effectively lead this global initiative, the United States should launch efforts to ensure that:

1. The United States and other donor states work together to fully meet humanitarian appeals, and significantly increase development investment in front-line refugee-hosting communities.

   - The United States, which recently pledged $925 million USD at the February 4, 2016 donor conference in London, should significantly increase its humanitarian assistance and development aid investments. Congress should support the necessary increases, including through any necessary increases in appropriations. The United States and other donors should emphasize that they expect front-line states to continue to allow refugees to cross their borders to access protection, to continue to host refugees, and to improve refugees’ access to employment and other basic rights and services.

   - In addition, the United States should intensify efforts to encourage other donor countries to increase development investment. U.S. and other development investment should focus on (i)
strengthening the key infrastructures of front-line communities that are hosting large numbers of Syrian refugees, including education, health care, and sanitation, and (ii) initiatives that will enable increasing numbers of Syrian and other refugees to work while also benefitting host communities.

- While not the subject of this report, the United States should continue to work with other states to press for humanitarian access to Syrian civilians trapped inside Syria in besieged areas and work to increase access to services as well as aid.

2. Protection in the Region—and at borders—is significantly strengthened so that refugees do not face the constant threat of rejection at borders, detention, deportation, lack of work permission and barriers to education.

- The president and secretary of state should redouble advocacy and champion the protection of the rights of refugees, including their rights to work, to access education and to cross borders in order to escape persecution and access effective international protection. Compliance with the refugee protection tenets developed in the wake of World War II, including international legal obligations to protect refugees fleeing persecution, is more important than ever, particularly at a time when thousands of families fleeing Russian bombs, Syrian government attacks, and ISIL terror have been blocked from escaping the violence raging within their country.

- Building on the recent announcement that Turkey will allow Syrian refugees to apply for work applications, the United States should work with other donor states to advocate for, and support initiatives that expand, the ability of refugees to work and access education in front-line refugee hosting countries.

- The United States should also ensure that NATO actions do not violate the human rights of refugees and migrants, including right of refugees to flee persecution and seek asylum. UNHCR has cautioned that NATO’s mission—which Secretary Kerry stated is to “close off a key access route” used by refugees and migrants in order to “stem this tide”- should not “undermine the institution of asylum for people in need of international protection.”

- If any “safe zone,” “no fly zone,” or similar proposals move ahead, the United States should strongly advocate that states surrounding Syria do not prevent refugees from crossing their borders in violation of customary international law prohibitions on refoulement. Safe zones in war-torn regions are notoriously unsafe for civilians.

3. Globally, states provide at least 460,000 resettlement and other admission places for Syrian refugees and the United States increases its commitment.

- The United States should increase its pledge for fiscal year 2017 to resettle 100,000 Syrian refugees, in addition to resettling refugees from other countries. Not only would such a commitment level be more responsive to the global need, but it would also advance U.S. national security, foreign policy, and humanitarian and human rights interests.

- The United States and other countries should increase support to UNHCR—through additional PRM funding—so the agency has greater capacity to identify and
refer cases for resettlement or other admission consideration.

4. Address staffing gaps to reduce backlogs and bottlenecks in resettlement and Special Immigrant Visa (SIV) processing, including:
   
   - **Increase Staff to Address DHS Backlog of Hold Cases Awaiting Review:** DHS should immediately increase staffing and resources to resolve the several thousand cases waiting their turn in no decision limbo for review by DHS officials. Additional staffing and oversight should also be provided to review cases waiting in the Controlled Application Review and Resolution Program (CARRP) hold backlog. The Obama administration and Congress should encourage and support this increase in staffing and resources, including through an appropriation of additional funding for DHS.
   
   - **Increase DHS and Vetting Agencies’ Staff and Resources to Address Backlogs in Resettlement and SIV Follow-up Inquiries:** The President should direct DHS and U.S. security vetting agencies to increase staffing and resources to conduct follow up vetting inquiries so the completion of security clearance vetting is not unnecessarily delayed—for either refugees or for SIV applicants—due to lack of sufficient staffing. Congress should encourage and support increases in staff and resources, including appropriation of additional funds for DHS and the security vetting agencies. These backlogs undermine the reputation of these programs and the country’s ability to meet its commitments to U.S. allies and refugee-hosting countries, to the international community and to vulnerable refugees and people facing grave risks due to their work with the United States. Addressing backlogs would strengthen the effectiveness and integrity of U.S. processing and would not undermine security. It is not in the security interest of the United States to have delays in security vetting, which would potentially delay identification of any individual who might actually present a security threat to this country or its allies in the region.
   
   - **Increase referrals to U.S. resettlement processing of vulnerable and U.S. affiliated Syrian refugees:** The U.S. Resettlement Program should move ahead robustly with priority processing for Syrian refugees with approved I-130 family petitions, engage with countries where U.S. processing occurs to assure that those with U.S. family ties can cross borders to actually access U.S. processing, and expand priority access to Syrian refugees (and their respective spouse and children) with relatives (at least spouses, children whether over or under 21 and whether married or unmarried, parents and siblings) in the United States who have any kind of lawful immigration status in the United States or have an application for such status pending.
   
   - In addition, the U.S. Resettlement Program should enlist and leverage trained and trusted non-governmental organizations to refer vulnerable refugee cases for U.S. processing, and encourage UNHCR to work closely with experienced non-governmental organizations that can assist in identifying and preparing cases. The State Department should also take steps to help expand UNHCR capacity to identify and refer cases for U.S. resettlement consideration. English as a second language classes should begin while
refugees are still in the region, during the long resettlement processing wait.

- **Increase U.S. resettlement processing at U.S. Embassy in Lebanon.** The U.S. Embassy in Lebanon should move ahead without delay on plans to expand capacity to host U.S. resettlement interviewers and processing. The president and secretary of state should make clear this expansion—and the accommodation of increased resettlement interviews in the meantime—is a top priority.

- **DHS should increase the size of the USCIS refugee corps and build on recent initiatives to conduct larger, more continuous, circuit rides to the region to minimize processing gaps and meet U.S. targets.**

- **The Departments of State and Homeland Security should continue to improve capacity to expedite resettlement, while conducting necessary security vetting, for particular individuals facing imminent risks of harm.**

5. **Create a high level assistant to the president charged with refugee protection:** The president should appoint a high level position at the White House to coordinate and ensure strong U.S. leadership of U.S. refugee protection efforts—across multiple U.S. agencies—to address the global refugee crisis, effective and timely U.S. resettlement and SIV processing, and the implementation of U.S. refugee protection commitments at home through the U.S. domestic asylum process and immigration system. Given the engagement of the U.S. military, including participation in NATO’s mission in the Aegean Sea, the United States will need strong mechanisms in place to assure refugee protection leadership globally and compliance with international legal standards. The senior official should have staff, including legal staff versed in international refugee conventions and U.S. human rights and refugee protection obligations. This official should also be charged with mapping out a plan for effective transition of leadership on these matters to the next U.S. administration. ■
Addendum

December 1, 2015

Dear Senator/Representative,

We write to express our opposition to proposals that would effectively halt the resettlement of Syrian and Iraqi refugees in the United States following the terrorist attacks in Paris. We believe that America can and should continue to provide refuge to those fleeing violence and persecution without compromising the security and safety of our nation. To do otherwise would be contrary to our nation's traditions of openness and inclusivity, and would undermine our core objective of combatting terrorism.

The process that refugees undergo in order to be deemed eligible for resettlement in the United States is robust and thorough. They are vetted more intensively than any other category of traveler, and this vetting is conducted while they are still overseas. Those seeking resettlement are screened by national and international intelligence agencies; their fingerprints and other biometric data are checked against terrorist and criminal databases; and they are interviewed several times over the course of the vetting process, which takes 18-24 months and often longer.

Given the stringent measures in place, we are especially concerned by proposals that would derail or further delay the resettlement of Iraqis who risked their lives to work with the U.S. military and other U.S. organizations. These refugees were given priority access to U.S. resettlement under the Refugee Crisis in Iraq Act. The United States has a moral obligation to protect them.

We must remain vigilant to keep our nation safe from terrorists, whether foreign or homegrown, and from violence in all its forms. At the same time, we must remain true to our values. These are not mutually exclusive goals. In fact, resettlement initiatives help advance U.S. national security interests by supporting the stability of our allies and partners that are struggling to host large numbers of refugees.

Refugees are victims, not perpetrators, of terrorism. Categorically refusing to take them only feeds the narrative of ISIS that there is a war between Islam and the West, that Muslims are not welcome in the United States and Europe, and that the ISIS caliphate is their true home. We must make clear that the United States rejects this worldview by continuing to offer refuge to the world's most vulnerable people, regardless of their religion or nationality.

Sincerely,

(Names in alphabetical order on following page)
Endnotes


7 UNHCR, Lebanon Briefing Kit, Jan. 2016.


13 Pamuk, Humeyra. "Faced with new influx, Turkey's open door for migrants may be closing." Reuters. (February 8, 2016).

14 Available at http://www.reuters.com/article/us-mideast-crisis-syria-turkey-migrants-idUSKCN0XH1DW.


16 HRF Interviews in Region. See also John Reed. "Syrian refugees stranded as Jordan blocks entry." The Financial Times. (January 18, 2016) available at http://www.ft.com/cms/s/0/30f22d4a-baa0-11e5-b151-8e15c9a029fb.html#axzz41EOaQ3QX.


19 UNHCR, Lebanon Briefing Kit, Jan. 2016.

For information on U.S. Resettlement Support Center Pre-Screening. Please see (1) Barbara Stack Testimony, FN 23; (2) USCIS submission - Hearing Before the Commission on Security and Cooperation in Europe (October 2015); (3) Testimony of

HUMAN RIGHTS FIRST

637
Lev Kubiak, USCIS, before the House Homeland Security Committee (February 2016) available

Testimony of Lev Kubiak, FN 19.

Interpol. "EU ministers call for access to INTERPOL’s databases at border points." (November 20, 2015) available at


Turkey’s Response to the Syrian Refugee Crisis and the Road Ahead, World Bank Group, (December 2015), available at https://www.openknowledge.worldbank.org/bitstream/handle/10986/23548/Turkey0a0respons0a0and0theroad0ahead.pdf?sequen ce=1&isAllowed=y at 7.


Respecting Rights and Securing Solutions

Recommendations for U.S. Leadership of a Comprehensive Initiative to Address the Global Refugee Crisis

August 2018
ON HUMAN RIGHTS, the United States must be a beacon. Activists fighting for freedom around the globe continue to look to us for inspiration and count on us for support. Upholding human rights is not only a moral obligation; it’s a vital national interest. America is strongest when our policies and actions match our values.

Human Rights First is an independent advocacy and action organization that challenges America to live up to its ideals. We believe American leadership is essential in the struggle for human rights so we press the U.S. government and private companies to respect human rights and the rule of law. When they don’t, we step in to demand reform, accountability, and justice. Around the world, we work where we can best harness American influence to secure core freedoms.

We know that it is not enough to expose and protest injustice, so we create the political environment and policy solutions necessary to ensure consistent respect for human rights. Whether we are protecting refugees, combating torture, or defending persecuted minorities, we focus not on making a point, but on making a difference. For over 30 years, we’ve built bipartisan coalitions and teamed up with frontline activists and lawyers to tackle issues that demand American leadership.

Human Rights First is a nonprofit, nonpartisan international human rights organization based in New York and Washington D.C. To maintain our independence, we accept no government funding.

© 2016 Human Rights First All Rights Reserved.

This report is available online at humanrightsfirst.org

ACKNOWLEDGEMENTS

We would like to thank The Oak Foundation, the Heising-Simons Foundation, the Herb Block Foundation, and the Libra Foundation, as well as general operating support from the Carnegie Corporation, MacArthur Foundation, and Bloomberg Philanthropies.

COVER PHOTO: REUTERS/Marko Djurica
Contents

Introduction .................................................................................................................................................. 1

Champion Compliance with International Law Prohibitions on Return or Rejection of Refugees ............................................................ 4

Meet Global Resettlement Appeals and Provide Other Orderly Routes to Protection ........... 7

Strengthen Respect for Rights to Work, Education, Liberty and Free Movement ............. 11

Fully Meet Humanitarian Appeals and Significantly Increase Development Investment and Support for Frontline Communities, Working with the World Bank, Other Donor States, Private Business, and Local Communities ................................................................. 13

Develop and Lead a Comprehensive Plan to Address the Syrian Refugee Crisis .......... 16

Endnotes .................................................................................................................................................. 20
**Introduction**

Two major summits slated for September 2016 present opportunities for the United States to lead, and advance key components of, a comprehensive initiative to address the global refugee crisis and champion the protection of the human rights of refugees and migrants. On the 19th the United Nations will hold a High Level Meeting on Refugees and Migrants, and on the 20th President Obama will convene a Leaders’ Summit on Refugees. In addition, the U.N. Secretary General has called on the world’s nations to develop two agreements to better address the needs and safeguard the human rights of refugees and migrants: the “Global Compact on Responsibility-Sharing for Refugees” and the “Global Compact for Safe, Regular and Orderly Migration.” In the wake of the failure of states to agree to an ambitious outcome document for the September 19 High Level Meeting, it is more important than ever for the United States to ensure that these opportunities are effectively leveraged to reinforce respect for human rights and the securing of solutions.

The number of refugees in the world has risen steeply in recent years and now exceeds 21 million. Nearly one in four has fled Syria; the number of Syrian refugees grew from about 20,000 in February 2012 to 4.8 million in 2016. Seventy-six percent of the global refugee population comes from just ten countries: Syria, Afghanistan, Somalia, South Sudan, Sudan, the Democratic Republic of Congo, Central African Republic, Myanmar, Eritrea, and Colombia. And ten countries—Turkey, Pakistan, Lebanon, Iran, Ethiopia, Jordan, Kenya, Uganda, the Democratic Republic of Congo, and Chad—host 58 percent of refugees. Several of these countries also host large numbers of Palestinian refugees. In many cases displacement has become protracted, the estimated duration of refugee situations now reaching 25 years on average up from 17 in 2003. For example, many Afghans have been displaced for decades and a third generation of Somali refugees is growing up in camps.

For the United States, resolving this global crisis is both a moral and national security imperative. In a June 2016 Statement of Principles on America’s Commitment to Refugees, a bipartisan group of former national security officials stressed that, “Accepting refugees, and encouraging other countries to do so, advances U.S. interests by supporting the stability of our allies struggling to host large numbers on their own.” In a December 2015 letter to Congress, a bipartisan group of former national security advisors, CIA directors, secretaries of Defense, Homeland Security, and State, said, “Resettlement initiatives help advance U.S. national security interests,” noting that refugees “are vetted more intensively than any other category of traveler.”

After World War II the United States helped establish an international system and legal framework grounded in the conviction that people fleeing persecution should never again be turned back to face horror or death. Today 148 nations are party to the U.N. Convention Relating to the Status of Refugees or its Protocol, including the United States, which is a member of the Executive Committee of the U.N. Refugee Agency (UNHCR). The United States is also a party to the International Covenant on Civil and Political Rights (ICCPR), which affirms the right to liberty and freedom from arbitrary detention.

Over the years the United States has often lived up to its ideals and its obligations, providing substantial levels of humanitarian aid and resettling more refugees than another country. Yet in the face of the current crisis, the country has fallen short. It has not launched and led a strong Syrian resettlement initiative to effectively support the frontline states surrounding Syria. Meanwhile
at home, it has implemented a detention-and-deterrence-based approach at its southern border—an approach that violates principles central to the global refugee protection system. During the negotiations on the outcome document for the September 19 High Level Meeting the United States proposed revisions to draft language on the detention of children that ran contrary to global human rights standards recognizing that detention is never in the best interests of children. When the United States falters in its obligations to refugees, it sends the wrong signal to other nations, encouraging rights-violating policies that exacerbate the global crisis. As U.N. Secretary-General Ban Ki-moon has pointed out, "This is not just a crisis of numbers—it is also a crisis of solidarity."

The international community should work harder to resolve the conflicts, human rights abuses, and violence that are causing displacement. Tackling the root causes should be a priority for this administration and the next, and for Congress. However, there is much that should be done to help refugees now.

This paper lays out key steps that the United States should take to lead a comprehensive effort to address the global refugee crisis. While the paper does not include every important action that the U.S. government should take to address the plight of refugees and migrants globally, it focuses on areas where U.S. action is vital. Most critically, the United States should champion the human rights of refugees. If basic human rights are not secured—including the rights to protection from return to persecution, the ability to work legally, and freedom from deprivations of liberty and arbitrary detention—refugees will continue to die, suffer, and struggle to rebuild their lives.

To truly lead by example, the United States and other nations should comply with international law. Like efforts to block Syrian refugees from crossing borders and the procedural and physical barriers erected by European states to impede and deter asylum seekers, the U.S. policy of holding families and others seeking asylum in detention facilities undermines the international refugee protection system and encourages other countries to evade their responsibilities. A strong recommittal to international refugee and human rights law is necessary not only to better help refugees, but also to pursue broader U.S. humanitarian, strategic, and national security goals.

The United States, as the single largest global humanitarian donor, is particularly well placed to work with other nations to advance U.S. goals for the Leaders' Summit with respect to increased humanitarian aid, development investment, support for education, and initiatives to increase the number of refugees granted legal permission to work. The United States should also lead—rather than lag—on the resettlement of Syrian refugees. While the specific U.S. goals for the Leaders' Summit have been narrowly defined, the United States should seize the opportunity to advance a more ambitious initiative to address the global refugee crisis, one that centers on securing state compliance with human rights and refugee protection legal obligations as well as solutions for all refugees.

In order to effectively lead such an initiative, in connection with President Obama's September Leaders' Summit, the U.N. High Level Meeting on Refugees and Migrants, and beyond, the United States should:

1. **Champion access to asylum and compliance with international law prohibitions against return or rejection of refugees, including:**
   - Strongly support adherence to international human rights and refugee law, ensuring that any global compacts or agreements reinforce, not weaken, legal protections with respect to
**nonrefoulement**, access to asylum, and the use of detention;

- Lead by example at home by ending border policies that block access to asylum, limit the use of expedited removal proceedings, abandon regional initiatives that block access to asylum, and support initiatives in the region that secure access to asylum;

- Encourage the states neighboring Syria to stop blocking refugees from fleeing their country, better support those states through resettlement and aid, and help Jordan transfer Syrians stranded in a dangerous desert area to safety so they can be screened and afforded access to asylum, resettlement, or protection;

- Call on the European Union to ensure access to asylum, cease mischaracterizing Turkey as a "safe third country," and halt deportations under its flawed deal with Turkey;

- Promote adherence to *refoulement* prohibitions, including with respect to Kenya's announcements on camp closure as well as the practices of Australia, Cameroon, China, Thailand, Malaysia, Indonesia, Vietnam, and other countries; and

- Ensure NATO activities comply with human rights and refugee protection law.

2. **Work with other nations to meet UNHCR's appeals to provide resettlement or other pathways to protection for 10 percent of the global refugee population, including:**

- Provide leadership through the doubling of the overall U.S. resettlement goal, urge European and other countries to substantially increase their resettlement efforts, and encourage South Korea to launch a resettlement program, Japan to expand its resettlement program, and Gulf nations—including Saudi Arabia and the United Arab Emirates—to allow Syrian refugees working in their countries to extend their stays and to be joined by family;

- Lead by example through a significant increase in the U.S. commitment to resettle Syrian refugees to a level of one hundred thousand (within a larger overall refugee goal), as recommended by a bipartisan group of former government officials, and at least to a level that corresponds to UNHCR's assessment that 40 percent of refugees in need of resettlement are Syrians;

- Expand U.S. resettlement initiatives for refugees from the Northern Triangle in Central America, and encourage other countries to do so as well;

- Launch a private sponsorship resettlement initiative in the United States and encourage European states to create such programs;

- Encourage that any global compacts or agreements on resettlement set a 10 percent goal consistent with U.N. assessments of resettlement need; and

- Continue to address staffing and efficiency gaps to reduce processing delays that hamper the effectiveness of U.S. resettlement and SIV initiatives.

3. **Strengthen respect for the right to work, education, liberty, and free movement, including:**

- Increase access to legal work authorization for all refugees, champion the right to work, and support front-line
states through assistance and development initiatives;

- Increase U.S. support for—and encourage other states to support—access to primary and secondary education as well as scholarships to universities;

- End U.S. detention policies that violate international law, including those relating to the detention of children and families, and encourage other nations to do so as well;

- Strengthen respect for the human rights of migrants globally and at home, including by supporting initiatives to improve compliance with applicable human rights law; and

- Support initiatives to protect refugees and migrants from xenophobic violence, prosecute perpetrators, and encourage the world’s leaders to condemn such incidents.

4. Partner with other nations to fully meet humanitarian appeals and lead a global effort to significantly increase development investment, and support frontline communities that host the overwhelming majority of refugees, working with the World Bank, other donor states, private businesses, and local communities.

5. Design and lead a comprehensive plan to address the Syrian refugee crisis. This plan should include a significant increase in resettlement by the United States and other countries, fully meet humanitarian appeals, promote major development investment to support refugee-hosting communities through a "Marshall Plan"-inspired initiative, and most critically, protect the right of refugees to cross borders, work, access education and be free from detention that is inconsistent with human rights standards.

---

**Champion Compliance with International Law**

**Prohibitions on Return or Rejection of Refugees**

"Even in time of desperation, we have to stick by our fundamental values, the rights that were drafted to protect people in vulnerable circumstances and conflict. When times are tough, governments sometimes look to cut corners. But that never works in the long term... It's critically important that governments around the world stay true to the letter and the spirit of the 1951 Refugee Convention and the 1967 Protocol; we need to see that in effect and not just on paper."

-Bono (Hearing before the U.S. Senate Appropriations Subcommittee on State, Foreign Operations, and Related Programs, April 2016)

Drafted in the wake of World War II and in the context of the many border restrictions that denied refuge to those fleeing Nazi persecution, the 1951 Refugee Convention and its Protocol prohibit states from *refoulement*, or returning people to places where their lives or human rights would be at risk. Even states that are not party to the Refugee Convention and Protocol must comply with this prohibition as it constitutes a tenet of customary international law.

The failure to adhere to these rules has not only left refugees in danger—for example, blocking families in Syria despite the threats of Russian bombs, Syrian government attacks, and ISIS terror—but it also makes clear to refugees that they cannot secure effective protection in the...
region surrounding their home country. The negative example of deterrence-driven and rights-violating policies adopted by some wealthier states will, if not remedied, undermine the global protection regime and the solidarity and responsibility-sharing necessary to address the global refugee and displacement crisis.

The United States should, among other steps:

- **Emphasize**—through both words and actions—that adherence to and respect for international law protections on *nonrefoulement*, access to asylum, and the safeguarding of the human rights of refugees and migrants is central to achieve the global community’s objectives to better manage the global refugee crisis and migration challenges.

- **Encourage Turkey, Jordan, Lebanon, Iraq, Egypt, and other states in the region surrounding Syria to comply with international law prohibitions against refoulement and stop blocking or preventing Syrians from fleeing their country.** Syria’s neighbors have already taken in large numbers of refugees, but many thousands more have been blocked from crossing to safety and are now trapped within Syria and in dangerous border areas.

In addition to encouraging these nations to comply with international law and allow Syrian refugees to cross their borders, the United States and other donor states should increase their support for frontline states hosting the majority of refugees through humanitarian aid, bilateral assistance, development investment, and resettlement. The countries that border Syria have legitimate security concerns, but these concerns can be addressed through individualized exclusion assessments conducted in accordance with international legal standards. In particular, the United States should help Jordan transfer Syrians stranded in horrendous conditions in the border area known as the “berm” to a safe location where they can be screened for security and protection purposes, and provided access to protection, including asylum or resettlement. In addition to conducting screening in Jordan, the United States should consider the use of other locations. For instance, the United States in the past has brought refugees to Guam and to Fort Dix in order to process their cases in a safe location.

- **Lead by example at home.** The United States should reform its own border policies by limiting the use of expedited removal, employing additional safeguards when that flawed process is used, and ending detention policies that violate U.S. refugee protection and human rights obligations, including the detention of families with children.

The United States should address the displacement of people from the Northern Triangle of Central America as a regional protection crisis, rather than treating the arrival of asylum seekers from that region as a political or border security crisis. It should refrain from employing punitive and harsh tools designed to “send a message” and “stem the flow.”

As UNHCR has urged, the United States should “ensure that all migration policies protect people’s legal right to seek asylum, and refrain from using detention as a deterrent.” Given the U.S. role as a global leader, its failure to champion the protection of refugees at home reverberates across the world.
discouraging other nations from welcoming and respecting the rights of those who seek protection at their borders. Policies of deterrence and detention put refugees at risk of further harm, exacerbate migration management challenges, and often deflect these challenges on to other, less wealthy nations.

- **Encourage the European Union to also adhere to refugee and human rights law and set a better example to the rest of the world.** By attempting to block refugees from reaching Europe, European states have not only violated and evaded their own obligations, but have also set a poor example to frontline states that host the vast majority of refugees. President Obama should call on the European Union to immediately implement safeguards and fair procedures to protect refugees from improper return, to reject the notion that Turkey is a “safe country” under refugee protection legal standards, and to cease deportations under the flawed E.U.-Turkey deal. Instead, the European Union should work with Greece and other nations to assure access to asylum, to open official border crossings where asylum seekers can receive security screening and be permitted to enter to apply for asylum, to ensure efficient relocation of asylum seekers to other E.U. member states, while at the same time expanding the resettlement of refugees from Turkey and other countries of first refuge to Europe Union states.

- **Ensure that any compacts or other agreements on refugees and migrants include a central component respect for their human rights, including commitments to adhere to**

refoulement prohibitions and to ensure access to asylum—including in connection with migration management, anti-smuggling, and maritime or other rescue or migration enforcement efforts—as well as commitments to provide and support access to the legal right to work, to education, to free movement, and freedom from detention that is inconsistent with human rights and refugee legal standards.

- **Ensure that NATO actions respect human rights law.** The United States should encourage and support increased search and rescue operations at sea, and also ensure that NATO actions—whether in the Aegean Sea or in the Mediterranean with respect to ships departing Libya or Egypt—do not violate the human rights of refugees and migrants, including the right of refugees to flee persecution and seek asylum.

Germany’s defense minister has said there is a “firm agreement” with Ankara that refugees rescued by NATO ships would “be brought back to Turkey.” UNHCR has cautioned that NATO’s mission in the Aegean Sea—which Secretary Kerry stated is to “close off a key access route” used by refugees and migrants in order to “stem this tide”—should not “undermine the institution of asylum for people in need of international protection.” Human rights experts focused on Europe have urged NATO to, in addition to saving lives at sea, facilitate the right to seek asylum by bringing asylum seekers safely to Greece or Italy.

- **Safeguard refugees at risk in Kenya.** The United States and the international community should continue to monitor the situation in Kenya, encourage the
government to comply with international refugee protection and human rights law, including to not return Somali and other refugees at risk of persecution and other harm. It should work to increase resettlement of refugees located in Kenya.

In early May, the Kenyan government announced plans to close refugee camps and called on UNHCR to assist in repatriations, noting that “rich” countries were limiting entry of refugees into their own borders. Following meetings with the U.N. Secretary General and the U.N. High Commissioner for Refugee, the Kenyan President said that Kenya would not "shy away from her international obligations" or return people “in a manner that defies their dignity, human rights or endangers their lives.” On June 25, a Tripartite Commission (Kenya, Somalia, and UNHCR) announced its aim to reduce the population at the Dadaab camp by 150,000 by the end of the year, including through voluntary returns, relocation of non-Somali refugees, and a population verification exercise.

- **Promote respect for non-refoulement and access to asylum in the western hemisphere**, including in Mexico, at the U.S. southern border, and in Central America, refraining from policies and funding activities that undermine international law through the support of migration "enforcement" without ensuring effective implementation of measures to safeguard access to asylum or other protection. In particular, the United States should ensure that funding for Mexican migration enforcement activities does not erode the right to seek asylum in Mexico and that any U.S. funding for Mexican border and immigration enforcement capacity is coupled with enhanced funding to improve and expand Mexico’s capacity to effectively identify, register, and process refugee and other protection claims, and to integrate recognized refugees and beneficiaries of complementary protection. The United States should work with UNHCR to support training and increased capacity for asylum systems in Costa Rica, Panama, Mexico, and other countries in the regions.

- **Encourage adherence to the Refugee Convention, Protocol, and international law prohibitions on refoulement** by all nations including Australia, Cameroon, China, Thailand, Vietnam, Malaysia, and Indonesia. The United States should prioritize in its advocacy with these and other nations engagement, advocacy, and support aimed at ensuring adherence to international legal protections against refoulement.

---

**Meet Global Resettlement Appeals and Provide Other Orderly Routes to Protection**

With over 21 million refugees globally, including over 4.8 million Syrian refugees, resettlement needs are acute. The United Nations has called on countries to commit to providing resettlement spaces or other legal pathways for admission to at least 10 percent of the global refugee population annually. UNHCR has estimated the global resettlement need for calendar year 2017 to be 1,190,000. In particular, given the significant needs and impact of the Syrian crisis on the
region surrounding Syria, UNHCR says 40 percent of the 1.2 million resettlement need for 2017 are for Syrian refugees. This is the highest level of resettlement need for Syrian refugees since the outbreak of conflict in the country in early 2011.

With respect to Syrian refugees alone, Oxfam calculated in its 2016 Syria Crisis Fair Share Analysis that the world’s richest governments had only pledged 129,966 resettlement or other humanitarian admission spots—still 350,034 below the overall Syrian resettlement need level of 480,000. The United States, long the global leader in resettlement, admitted only 105 Syrian refugees in fiscal year 2014 through resettlement, only 1,682 in fiscal year 2015, and as of July 31, 2016, has admitted 7,551, about 75 percent of its commitment to resettle ten thousand Syrian refugees in fiscal year 2016.

U.S. national security experts have repeatedly emphasized—in various bipartisan letters, statements, and op-eds—that responsibility-sharing through resettlement and other orderly admissions helps to relieve some of the pressures on frontline states that often host the overwhelming majority of refugees. In addition, as the U.N. Secretary General noted, "These alternative pathways provide viable alternatives to irregular and often dangerous journeys."

The lack of effective resettlement or other orderly routes to protection also have significant negative consequences. As detailed in Human Rights First’s February 2016 report, based on research in Jordan, Lebanon, and Turkey, the lack of effective regional protection, exacerbated by the lack of assistance and insufficient orderly resettlement or visa routes for refugees, has driven many Syrian refugees to embark on dangerous trips to Europe. In Turkey primarily, and also in Jordan and Lebanon, Human Rights First researchers heard reports that refugees who had been struggling to survive for years in exile lost hope in waiting for potential resettlement and decided to instead take the dangerous trip to Europe.

At its September 2016 Leaders’ Summit on Refugees, the United States has indicated that it will seek firm and explicit commitments from governments to provide additional resettlement or other pathways for refugees in need of international protection and will seek to double the number of resettlement or other admission spots made available globally for refugees.

The United States should, among other steps:

- Encourage nations to work collectively to meet the global ten percent refugee resettlement and other pathways goal and provide leadership through doubling of the overall U.S. resettlement goal. The United States should work with other nations to, collectively, meet the ten percent target and should call for this goal to be central to any compact on responsibility-sharing, along with a framework for dividing up responsibility among states. The United States, long the global leader in refugee resettlement, is particularly well placed to encourage other nations to initiate resettlement programs or to increase the size of their resettlement initiatives as well as other orderly admissions commitments such as labor visas, family unity, educational scholarships, labor visas, medical evacuations, and other humanitarian pathways. To provide strong leadership, the United States should double its own resettlement goal for fiscal 2017, from on hundred thousand to two hundred thousand, and encourage other nations to double or more substantially increase their resettlement initiatives.

The United States should encourage European nations to significantly increase

HUMAN RIGHTS FIRST

652
their resettlement initiatives. In addition, the United States should encourage South Korea to launch a resettlement program, encourage Japan to dramatically increase its resettlement program, and encourage Gulf nations—including Saudi Arabia and the United Arab Emirates—to allow Syrian refugees working in their countries to extend their stays and to be joined by their families.

- **Lead by example and substantially increase the U.S. commitment to resettle Syrian refugees.** A bipartisan group of former U.S. government officials, including ones with national security and humanitarian expertise, have called on the United States to resettle one hundred thousand Syrian refugees, over and above the worldwide U.S. refugee goal. Such a commitment would, they said, "send a powerful signal to governments in Europe and the Middle East about their obligations to do more." The Bipartisan U.S. Commission on International Religious Freedom, explaining that "[t]he United States must continue to live up to our nation's core values," has similarly recommended that the United States resettle one hundred thousand Syrian refugees.

For fiscal year 2017, the U.S. government should, in addition to resettling roughly one hundred thousand refugees from other countries, aim to resettle one hundred thousand Syrian refugees, a commitment more commensurate with both the American tradition of leadership and U.S. national security interests. This commitment level would be modest compared to Jordan, Lebanon, and Turkey, and would amount to just over two percent of the overall Syrian population hosted by these and other states in the region—and only about 21 percent of the overall Syrian resettlement need. This commitment would still fall far short of the U.S. "fair share" level of 170,779 Syrian resettlements. At the very least, the United States should allocate 40 percent of its resettlement slots to Syrian refugees given UNHCR's assessment that 40 percent of global resettlement needs are for Syrians.

A group of former national security advisors, CIA directors, secretaries of state, and Department of Homeland Security secretaries, who served under both Democratic and Republican administrations, pointed out that "resettlement initiatives help advance U.S. national security interests by supporting the stability of our allies and partners that are struggling to host large numbers of refugees," and also stressed that refugees "are vetted more intensively than any other category of traveler."

- **Launch resettlement for refugees from the Northern Triangle.** The United States should encourage and support resettlement initiatives for refugees from the Northern Triangle of Central America, building on its July 2016 announcement on the launch of a U.S. resettlement effort from the region. The United States should encourage Mexico and other refugee-hosting states in the region to work with UNHCR to launch resettlement initiatives, lead in accepting resettled refugees through such initiatives, and encourage Canada and countries in Latin America to accept Northern Triangle refugees through such initiatives.

The United States should also improve its program for resettlement of Central
American children by improving the interview and review process for the existing Central American Minors (CAM) program and by expanding the types of relationships that can serve as qualifying relationships, such as opening the program to children with adult relatives who are lawfully present in the United States, not just those with lawfully present parents.

The United States should expand its capacity to conduct emergency evacuations for refugees, including children, at risk of immediate harm and should adjudicate their claims for refugee status and/or parole as quickly as possible. The United States should launch its own resettlement initiative for refugees from the Northern Triangle, and this initiative should be commensurate with the regional resettlement needs. (Any and all resettlement efforts should make clear, including to U.S. asylum adjudicators, that resettlement is not a substitute for asylum.)

- **Affirm that resettlement and other orderly admission routes are not a substitute for access to asylum and compliance with international law.** Any and all compacts, agreements, or plans to increase resettlement must make clear that resettlement and other orderly admission routes are not a substitute for access to asylum and adherence to non-refoulement legal obligations.

- **Continue to address staffing and efficiency gaps to reduce backlogs and bottlenecks in the U.S. resettlement and SIV processing.** The Department of Homeland Security, Department of State, and other agencies should continue efforts to increase staffing, efficiency, prioritization, and resources to address the backlogs, delays, and efficiency gaps that are hampering the U.S. resettlement process. The president and Congress should encourage and support increases in staff and resources.

These backlogs undermine the reputation of these programs and the nation’s ability to meet its commitments to U.S. allies, other refugee-hosting countries, and vulnerable refugees, including those facing grave risks due to their work with the United States. Addressing delays, backlogs, and efficiency gaps would not undermine security; rather it would strengthen the effectiveness of U.S. processing. It is certainly not in the security interest of the United States to have delays in security vetting, which would potentially put off the identification of a person who might actually pose a security threat.

- **Launch private sponsorship initiatives.** The United States should enhance its resettlement capacity through a private sponsorship initiative that would allow family members and other U.S. groups, corporations, charities, and individuals to support with private funds the resettlement of additional refugees to the United States, above and beyond the U.S. government’s yearly goals.

It should launch a pilot program immediately that builds upon the existing resettlement framework and expertise and provides an opportunity for citizens to directly engage and to fund private resettlement to bring additional refugees. The Canadian government has successfully operated a privately sponsored resettlement initiative for many years, and the United States operated a
private sponsorship program under the Reagan Administration. The United States should also encourage European states to launch private sponsorship programs. These initiatives should supplement—not substitute for—robust state funded resettlement initiatives.

**Strengthen Respect for Rights to Work, Education, Liberty and Free Movement**

Under international law, refugees are entitled to key human rights protections, including the right to work, to education, and to liberty and free movement. The deprivation of these rights often leaves refugees with little choice but to seek protection in other countries.

For instance, in research conducted in Jordan, Lebanon, and Turkey earlier this year, Human Rights First researchers heard—again and again—that refugee-hosting states had denied refugees the ability to work legally, that refugee children faced tremendous barriers to education, and that refugees were facing increasing risks of exploitation, detention, and deportation in the face of increasingly harsh government policies and registration requirements.

Without protection of their basic rights—including protection from return to persecution, the ability to work legally, effective access to education, and freedom from arbitrary detention—many refugees believed they could not safely remain and rebuild their lives in the region. And many made the difficult choice to embark on dangerous journeys to seek protection in Europe. Alternatively, by assuring adherence and access to these rights the global community can advance its broader goals.

Using detention against asylum seekers and migrants is a growing global human rights abuse. Numerous human rights and other reports have documented the abusive detention policies used by various nations including Australia, Canada, Greece, Israel, Thailand, South Africa, and the United States.\(^9\)

In addition, the United States and several other countries hold children with their families in immigration detention, contrary to international law prohibitions and restrictions on the detention of children.\(^10\) The United States, which has 3,028 beds in detention facilities for families, has detained babies and their nursing mothers as well as young children and their families.

The United States should, among other steps:

- **Champion self-reliance and the right to work.** Any compact or agreements generated in connection with or after the September U.N. High Level Meeting and U.S. Leaders’ Summit should recognize existing rights to work, commit states to complying with these rights requirements, and commit donor states and others to supporting access to those rights including through investment initiatives.

The United States should encourage Turkey, Jordan, Lebanon, Egypt, and other countries to allow refugees to work to support themselves. The United States has set as its goal for the Leaders’ Summit to increase by one million in the number of refugees globally granted the legal right to work. The United States should expand this goal going forward. As outlined below, the United States should also take steps to increases jobs for refugees and host-communities, enlisting business leaders, financial institutions, and governmental and private donors and should encourage the European Union,
Gulf States, World Bank, and business leaders to support work initiatives.

- Increase funding for, and access to, primary and secondary education as well as scholarships to universities. The United States has set as its goal for the Leaders’ Summit to increase the number of refugees in school by one million. The United States should encourage donor states and private donors to expand support for initiatives that increase opportunities for refugees to access education while also supporting refugee hosting communities through university scholarships for refugees. An initiative that offered 70 university scholarships for Syrian refugees in Turkey prompted five thousand applications. The United States should encourage and fund the creation of similar programs, and urge other nations to do so as well.

- End and limit the use of migration detention that is inconsistent with human rights and/or refugee law, including with respect to asylum seekers and children. Any compacts or agreements relating to refugees or migrants must affirm adherence to international human rights and refugee law limits on the use of migration detention. The United States should encourage Australia, Canada, Greece, Israel, South Africa, Thailand, and other nations to end migration detention policies that violate international human rights and/or refugee law. The United States should use and encourage alternative measures (such as community-based case management programs) rather than detention when additional support is needed in an individual case to ensure court appearance. Detaining asylum seekers is generally impermissible under the Refugee Convention, Protocol, and human rights law, and is particularly problematic when it exceeds a few days.

- Reform U.S. policies to safeguard children, asylum seekers and other immigrants from detention that violates international human rights and/or refugee law. The United States should lead by example, and in particular should end its failed policy of holding families seeking asylum in immigration detention, eliminate “mandatory” detention policies, provide prompt court review of detention for “arriving” asylum seekers and other immigration detainees, and use alternatives to detention (such as community-based case management programs) when additional measures are needed to ensure that an individual appears for immigration appointments.

- Reform U.S. policies to assure access to work and education. The United States must also address the substantial staffing gaps that are delaying its ability to adjudicate asylum cases (both before the USCIS asylum division and the immigration courts), and in turn delaying access to family unity, stable work opportunities, and some education opportunities. The United States should also provide earlier access to work authorization for asylum seekers.

- Strengthen respect for the human rights of migrants. The United States should support, and call on other nations to support, the development of tools and mechanisms to improve compliance with international human rights law applicable to migrants. These include guiding principles and other measures outlining the many existing provisions of
international law and conventions that apply to migrants. The United States should also support initiatives to bring national laws and practices into compliance with human rights law.

In addition, the United States should urge that any compacts or agreements among states relating to migration must be grounded in, and affirm compliance with, existing human rights law applicable to migrants; and that, as the International Organization for Migration (IOM) is integrated into the United Nations, it be given an official human rights protection function and such function should be reflected in its Constitution.

- Support initiatives to protect refugees and migrants from xenophobic violence. U.S. law enforcement authorities must closely monitor xenophobic incidents and prosecute bias-motivate crimes. U.S. political leaders must speak out strongly against any such incidents as well as against xenophobic statements.

The United States should also support initiatives in Europe, Africa, and elsewhere that are aimed at protecting refugees and migrants from xenophobic violence, share law enforcement experience and training, fund initiatives that assist refugee and migrant communities to report such violence to the authorities, and encourage leaders in refugee-hosting countries to speak out against attacks on refugees and migrants. The United States should work with the Organization for Security and Co-operation in Europe (OSCE), UNHCR, and other donor and refugee-hosting nations to galvanize and secure support for these initiatives.

Fully Meet Humanitarian Appeals and Significantly Increase Development Investment and Support for Frontline Communities, Working with the World Bank, Other Donor States, Private Business, and Local Communities

“Our foreign assistance strategy and programs must place greater emphasis on catalyzing and supporting economic growth and opportunity ... [I]n this new era of human development, entrepreneurs, investors, and innovators are as fundamental to geopolitical stability as politicians, generals, and diplomats; and trade and investment agreements are as instrumental to world order as defense pacts.”

—General James Jones, retired

While the United States has been a strong leader in providing humanitarian aid, the gaps between need and resources are growing. The $10.2 billion funding gap for 2015 was the largest on record, with only 49 percent of U.N. humanitarian appeals met. The gaps in UNHCR funding last year—at about 50 percent of its budget needs—led to cost cutting measures throughout the year, forcing the agency to “make very difficult choices, some a matter of life and death.”

Just under 50 percent of UNHCR’s appeals for the Syria crisis went unfunded as well. By the middle of 2015, financial shortages had forced the World Food Programme to reduce its assistance to 1.6 million Syrian refugees in five countries.
The food assistance cuts—as one aid worker in Jordan told Human Rights First researchers—had a “domino effect” on refugee families, impacting not only their ability to eat but their ability to pay rent. Some felt they had no choice but to withdraw children from school so that the children could work to help support their families. Others felt they had little choice but to head to Europe in order to secure their survival.

As of April 2016, only 19 percent of the U.N. Coordinated Appeals for 2016 have been met. Only 23 percent of the Syria Humanitarian Response Plan and only 37 percent of the Syria Regional Refugee and Resilience Plan for 2016 have been met as of July. UNHCR reported in April that its programs in Africa were at a breaking point, with only about 35 percent of the needs met. A major donor conference for the Syria crisis, held in London on February 4, 2016, led to over ten billion dollars in humanitarian and development “pledges” of assistance for the crisis. But most of this pledged assistance has not yet been delivered. 12

In his May 2016 report, the U.N. Secretary General stressed that the international community must, in addition to addressing humanitarian needs, also “expand development funding from the outset of displacement to address refugee needs and reinforce the national institutions, services and communities that support them.” He explained:

It is imperative that humanitarian and development actors work together with receiving States and identify common outcomes that both can support, including the reduction of dependency on international humanitarian aid over time in favor of more sustainable solutions .... [G]iven the average long length of displacement, the response will be more sustainable if it builds on national and local systems and incorporates a development approach, even in the early stages of an emergency.

The president of the World Bank, Jim Yong Kim, has stressed that the world’s powers need to pay greater attention to boosting economic growth and creating jobs in fragile countries to avoid even greater refugee crises in the coming years. In an April 2016 speech he called for major shifts in the way the World Bank works, including “investing and supporting middle-income countries that face the challenge of fragility, especially when the spillover effects from fragility can threaten both its neighbors and countries on the other side of the earth. If we leave these problems unresolved, the risk of growing conflict and extremism in these contexts will become very real as we have seen in the Middle East, North Africa and Latin America.”

The Middle East Investment Initiative has similarly warned, “The impact of the refugee crisis means that additional strain has been placed on already weak economic institutions and ignoring these economic and labor market challenges will have severe global security and political ramifications.”

A number of voices have called for a “Marshall Plan” approach to development investment in refugee-hosting states. Some of these proposals are focused globally, and others more specifically on the Middle East.13 U.S. non-governmental organizations have urged the United States to work with its allies and with the United Nations to lead in developing and funding a “comprehensive recovery and support plan” for Syria and its neighbors, “mirroring the scale and commitment of the Marshall Plan instituted to repair war-torn Europe, to meet the urgent needs of refugees in the region and foster their resilience.” These organizations urged that the plan “move beyond humanitarian emergency relief to include sustainable development projects, education, livelihood programs, and reconstruction.”14

Senator Lindsey Graham, after a visit to the Middle East in April 2016 also called for a new
“Marshall Plan” to provide billions of dollars to the region, potentially through an emergency appropriation.

In calling for a “Middle East Recovery Plan,” the Middle East Investment Initiative explains:

The Middle East in 2015 is not Europe in 1948, but the general principles of assistance to accomplish a joint recovery program based on self-help and mutual cooperation still apply. There is a tendency to shy away from any reference to the Marshall Plan due to its cost (an estimated US $160 billion in today’s US dollars). But the original Marshall Plan was not entirely based on financial aid. It also strengthened institutions and focused on private sector economic growth. In the Middle East, aid is needed to deal with the immediate crisis, but so, too, are measures to promote long-term investment in the economy and security of the region. The establishment of strong economic institutions and dynamic public-private partnerships, key components of the original Marshall Plan, will be critical to long-term sustainable development in the Middle East as well.\(^15\)

As part of a comprehensive plan to address the global refugee crisis, the United States should:

- **Work with other donor states to fully meet humanitarian appeals and significantly increase U.S. humanitarian aid and development investments in frontline refugee hosting states, initiating development investment much earlier.** In particular, with Congress’s support, this administration and the next administration should substantially increase both U.S. humanitarian assistance for Syrian refugees and displaced persons and U.S. development aid for refugee-hosting communities. The United States should leverage this leadership to push other states to increase their contributions as well so that global aid appeals are fully met.

The U.S. goal of securing a 30 percent increase in aid through the Leaders’ Summit in September is a step in the right direction, but additional action is needed. In particular, the United States and other donors should expand and replicate initiatives that increase opportunities for refugees to work and access education, while also supporting refugee-hosting communities. The U.N. Secretary General has urged that “local and civil society partners and NGOs must be supported by donors and international organizations to play a greater role in humanitarian responses.”

In April 2016, a group of former Senators, both Democrats and Republicans, urged that the United States keep pace with growing global challenges, including the historic refugee crisis in the Middle East, rather than cutting the International Affairs budget. They pointed out, “Strategic investments in development and diplomacy are crucial to advancing our national security and economic interests while ensuring a more secure and stable world,” and that “these programs are cost-effective investments that enable the United States to support allies like Israel and Jordan, respond to humanitarian crises, and promote U.S. interests abroad.”\(^16\)

- **Encourage development agencies to prioritize refugee and displacement situations.** The United States and other nations should encourage their development agencies to prioritize or further prioritize initiatives aimed at
addressing refugee and displacement situations. Such initiatives should not be limited to funds traditionally allocated to “refugee” situations, but should be integrated and prioritized throughout such agencies.

- **Prioritize development support for key public infrastructures.** Donor states and financial institutions should also prioritize development investments that improve public infrastructures impacted by hosting refugees, and increase the overall housing stock, health and education services, and income-earning opportunities that can best benefit both host communities and refugee populations.

- **Continue to encourage greater engagement and investment by private donors, investors, and businesses to better support refugees.** The United States should continue its efforts to encourage private donors, investors, and businesses to contribute to humanitarian appeals and to strategically invest in refugee-hosting states in ways that support both refugees and refugee-hosting communities. The United States should also encourage incentives to promote such investments.

- **Encourage continued focus by the World Bank and other institutions on refugees and displacement.** The United States should encourage the World Bank’s continued focus on the global refugee and displacement crisis, including through innovative financing instruments, concessional loans to countries hosting refugees, and the development of Special Economic Zones.

For instance, the World Bank decided to offer Jordan, a middle-income country, the rates that had previously been reserved for the poorest countries, because of Jordan’s role in hosting Syrian refugees. The bank provided a one hundred million dollar loan at low concessional rates and plans to provide an additional two to four hundred million dollars in concessional financing in order to build special economic enterprise zones, which will aim to create thousands of jobs for both Syrian refugees and Jordanians over the next five years. The World Bank’s president has urged that this new approach “must now be taken to scale and implemented in other countries as well.”

- **Lead a “Marshall Plan”-inspired global strategy to spur economic growth in countries hosting refugees,** in particular with respect to the Syrian refugee crisis as described under recommendation five below.

---

**Develop and Lead a Comprehensive Plan to Address the Syrian Refugee Crisis**

The United States and the global community must focus greater attention on addressing the Syrian refugee crisis. Nearly one-fourth of the world’s 20 million refugees are from Syria. As a bipartisan group of prominent U.S. former national security officials recently stressed, “Accepting refugees, and encouraging other countries to do so, advances U.S. interests by supporting the stability of our allies struggling to host large numbers on their own.”
Moreover, as noted earlier in this paper, the international community’s failure to adequately support refugees and frontline countries hosting Syrian refugees drove many to embark on dangerous journeys to seek protection in Europe.

The critical components of a comprehensive plan to address the Syrian refugee crises should include increased resettlement, stepped-up humanitarian aid and development investment, as well as advocacy, diplomacy, and engagement focused on securing the rights of refugees to cross borders to access protection, to work, to access education, and to be free from detention that violates international refugee or human rights law.

As part of such a comprehensive plan, the United States should:

- **Champion the rights of refugees, including their right to cross borders, to work and to access education.** The United States should encourage Turkey, Jordan, Lebanon, Iraq, Egypt, and other states in the region surrounding Syria to comply with international law prohibitions against *refoulement* and stop blocking or preventing Syrians from fleeing their country, as outlined in recommendation section one above.

  The United States should encourage Turkey, Jordan, Lebanon, Egypt, and other countries to allow refugees to work to support themselves. For instance, Turkey—which hosts 2.8 million Syrian refugees—should adjust its new work authorization rule for refugees, including to allow other refugees to access work authorization (in addition to Syrian refugees), and to eliminate the ten percent limitation on the number of Syrians in any given workplace. The CATO Institute has recommended that

  the Turkish government increase or entirely remove its ten percent cap on Syrian employment. The United States should also increase funding for, and access to, primary and secondary education as well as scholarships to universities.

- **Work with other donor states to fully meet humanitarian appeals and significantly increase U.S. humanitarian aid and development investments in frontline refugee hosting states,** as outlined in recommendation four above.

- **Lead a “Marshall Plan”-inspired global strategy to spur economic growth in countries hosting Syrian refugees.** The United States should lead the international community—including Europe, the Gulf Cooperation Council, other G20 countries, international organizations, and the private sector—to create a sustainable global economic strategy that commits resources and technical assistance to spur economic growth in the countries hosting Syrian refugees.

  The Middle East Investment Initiative recommends that a Middle East Recovery Plan (MERP) focus on strengthening economic and financial institutions that will help expand economic opportunity in the private sector in Turkey, Jordan, and Lebanon. It urges that, to be sustainable, this effort should build economic vitality from the bottom up, allowing entrepreneurs to flourish and small and medium-sized enterprises in the region to grow. It will require partnerships and alliances with international and local governments, the private sector, and civil
society—including Syrian refugees and organizations.

The Middle East Investment Initiative notes that this growth will require capacity building and investments in local governments, financial institutions, and the private sector. Its recommendations detailed in its April 2016 proposal include: alternative financing instruments that can support and promote private sector engagement strategies involving local as well as international private sector partnerships; technical assistance and direct financing to micro and small-medium enterprises; and providing direct financing and technical assistance to local organizations and entrepreneurs delivering essential services to refugee communities.19

The organization also notes that a coordinated international proposal for a Middle East Recovery Plan is sustainable only if existing laws and barriers to legal employment and work permits for refugees are addressed.

■ Substantially increase the U.S. commitment to resettle Syrian refugees and encourage other states to step up their resettlement and admission of Syrian refugees. As outlined earlier in these recommendations, the United States should aim to resettle or provide other admission routes for one hundred thousand Syrian refugees over the next fiscal year, a commitment level that is more commensurate with both the American tradition of leadership and U.S. national security interests. This commitment level would be quite modest compared to that of Jordan, Lebanon, and Turkey, and would amount to just over two percent of the overall Syrian population hosted by these and other states in the region, and only about 21 percent of the overall resettlement need. This commitment would still fall far short of the U.S. “fair share” level of 170,779 Syrian resettlements. At the very least the United States should allocate 40 percent of its resettlement slots to Syrian refugees given the UNHCR assessment that 40 percent of global resettlement needs are for Syrian refugees.

The United States should also encourage European states to significantly increase their resettlement of Syrian and other refugees, and should encourage Gulf nations—including Saudi Arabia and the United Arab Emirates—to allow Syrian refugees working in their countries to extend their stays and to be joined by family.

A group of former national security advisors, CIA directors, secretaries of state, and Department of Homeland Security secretaries, who served under both Democratic and Republican administrations, has pointed out that “resettlement initiatives help advance U.S. national security interests by supporting the stability of our allies and partners that are struggling to host large numbers of refugees,” and also stressed that that refugees “are vetted more intensively than any other category of traveler.”

■ Don't use “safe zones” to block escape and deny refugees the right to flee. If any “safe zone,” “no fly zone,” or similar proposals move ahead with respect to Syria, the United States should strongly advocate that states surrounding Syria do not use the existence of any such zones as an excuse to deny access
to, or push back, refugees in violation of international law prohibitions on *refoulement*. "Safe zones" in war-torn regions are notoriously unsafe for civilians. The United States should continue to press for access to international protection and respect for the prohibition against *refoulement*. Any proposals to protect civilians inside Syria should also respect these essential rights.
Endnotes


8 The United States government obtains significant amounts of information about, and rigorously vets, Syrian refugees resettled to the United States, who come primarily from Jordan and Turkey where they have been struggling to survive for years. This vetting is the most rigorous of any travelers to the United States. It entails multiple interviews and involves numerous U.S. and international intelligence and law enforcement agencies, including the National Counterterrorism Center, the Department of Defense, and Interpol, which have extensive databases on foreign fighters, suspected terrorists, and stolen, false, and blank passports from Syria, Iraq, and elsewhere. This vetting includes access to information provided by many other countries, including those in the region surrounding Syria. See endnote 5, supra, and Human Rights First, "Refugee Resettlement Security Screening Information." Available at: http://www.humanrightsfirs.org/resource/refugee-resettlement-security-screening-information.


HUMAN RIGHTS FIRST
RESPECTING RIGHTS AND SECURING SOLUTIONS  21


Global Crises Are Overshadowing Hate Crimes

Jonathan A. Greenblatt  @JGreenblattADL  Elisa Massimino  @ecmassimino  May 5, 2016

Greenblatt is CEO and National Director of the Anti-Defamation League.

Elisa Massimino is the President and Chief Executive Officer of Human Rights First.

The lack of action is unacceptable

In the shadows of global crises, it’s a sad fact of everyday life that people around the world are routinely attacked, threatened or intimidated simply because of who they are or what they believe. In addition to the impact on individuals, these attacks, left unchecked, metastasize and grow—sometimes to crises. Governments can and should do much more to document, prevent and punish these bias-motivated crimes.

Hate crimes have a uniquely devastating emotional and psychological impact; they terrorize not only the direct victims, but entire communities. When employees of a Kosher deli in Copenhagen came to work last April to find broken glass and the word “Judenrein,” (Jewish pig) written on the wall, a whole community was threatened. When, in December, a man beat a Muslim storeowner in Queens in broad daylight, declaring, “I kill Muslims,” other Muslims and people perceived as Muslims feared for their safety. These crimes reflect the persistence—and in some cases, the resurgence—of xenophobia, antisemitism, Islamophobia and other forms of bigotry in Europe and the U.S.
In Europe, the increasing strength of both far-right political parties and Islamist extremists has created a dangerous environment for minorities. Antisemitism is the virulent thread linking the ideologies of these groups, and each is exploiting the refugee crisis for their own purposes. Far-right parties use it to stir up hatred against Muslims and immigrants; Islamist extremists cite this hostility as proof that Muslims have no place in the West to fuel recruitment to their ranks. And in many parts of Europe, other groups—such as Roma and LGBT people—are frequent targets of violent hate crimes.

The world's largest regional security organization, the Organization for Security and Cooperation in Europe (OSCE) is a leader in addressing this problem. It collects data from governments and nonprofit organizations on hate crimes across its 57 member states, including Russia and the U.S.

Every year, the Anti-Defamation League and Human Rights First team up to grade OSCE countries on their efforts to track and address hate crimes. The verdict? Despite their
arsenal of commitments, training programs and tools, most OSCE countries are failing to respond adequately to hate crimes, leaving minority communities in danger.

Bias-motivated attacks are difficult to track. But statistics suggest that once every 90 minutes in the U.S. someone—or some business or institution—is attacked because of personal characteristics; in the E.U., with a much larger population, the frequency is even higher. For many LGBT people, Muslims, Roma, Sinti, Jews and other vulnerable communities in the OSCE region, avoiding violence and harassment informs daily lives. Commitments to human dignity and fundamental rights ring hollow without action to confront this problem. Even in countries where governments are taking significant action, such as France, Germany and the U.K., Muslims face restrictions on their right to wear headscarves in public spaces, and harassment is so prevalent that some Jews question whether it is safe to wear a kippah in public.

Given the severity of this problem, the lack of serious commitment from many OSCE countries is an astonishing dereliction. While 52 of the 57 countries have a hate crime law or sentencing-enhancement law on the books, only about half report more than one hate crime per year. Even fewer countries report specific data—the type of crime, the target or whether the perpetrator is punished. Even more troubling, 21 governments didn’t collect any data at all. NGOs, with virtually no resources or reach, report a vastly more disturbing picture.

This is unacceptable. Without comprehensive information about the nature and magnitude of hate crime, efforts to combat it will be hobbled, at best. While the problem of underreporting and incomplete hate crimes laws is not unique to Europe, and the U.S. faces its own challenges in extending fully inclusive hate crimes laws to all 50 states, for the sake of their citizens and societies, European governments should make good on their own commitments to combat hate crime. Tracking the problem is an essential first step.

Hate crimes are corrosive. Left unaddressed, they lead to broader society breakdown and increased violence. Communities and individuals victimized by bias-motivated violence shouldn’t be left to fend for themselves. Advocates of equality everywhere should demand that governments take hate crimes seriously. We all have a stake in building societies that are intolerant of intolerance.
Op-Ed

The Syrian Refugee Crisis Won’t Be Solved With Small Gestures

Jonathan A. Greenblatt, National Director of the Anti-Defamation League, and Elisa Massimino, President and CEO of Human Rights First

This article originally appeared in MSNBC.com on September 30, 2015

The image of three-year old Aylan Kurdi washed ashore on a Turkish beach provoked the conscience of the world. But photos don’t resolve crises—leaders do. The plight of Syrian refugees—caught between Assad’s barrel bombs and ISIS’s medieval brutality—is a defining moment for American leadership. How we respond will resonate in the region and around the world for decades to come.

Given its proximity to Syria, Europe has a responsibility to help. This is certainly a political challenge on a continent where neo-fascist parties have ascended by stoking anti-immigrant sentiment, and some governments—Hungary, most notably—have responded with hostility. Thankfully, the German government is defying the demagogues, pledging to welcome 500,000 Syrians a year.

Even that, however, will not be enough. Our organizations represent victims of persecution and terrorism, and we know from experience that a problem of this magnitude and complexity can’t be solved by piecemeal approaches. The largest refugee crisis since World War II demands a coordinated global response, and that will not happen absent sustained American leadership.

Last week, the Obama administration submitted its refugee resettlement numbers for next year: and these will be the topic of a Senate Judiciary subcommittee hearing. Its commitment to resettle at least 10,000 Syrians and to raise the overall number of refugees to be resettled by 15,000 is welcome—but inadequate. Our country should be helping many more, given its capacity and legacy of leadership.

That’s not to say America’s record is unblemished. Politics and bigotry have too often influenced life and death decisions about who gets safe haven, and who is left to the wolves. A particularly dark stain came in 1939, when President Roosevelt bowed to pressure and denied safe haven to a boatload of Jews fleeing Nazi Germany. The St. Louis was forced back to Europe, and 254 of its passengers perished in the Holocaust.

After World War II, the world community agreed—with the 1951 UN Refugee Convention and Protocol—that refugees should never again be returned to persecution. Providing safe haven is a fundamental responsibility of democratic nations—grounded in international law and basic decency—and the U.S. has mostly been at the forefront of the effort to help refugees find it.

Presidents of both parties have led major initiatives to resettle refugees to the U.S. Some 400,000 Eastern Europeans came here after World War II, and our country welcomed more than 800,000 Cubans after Castro came to power. In 1975, President Ford overcame resistance to set up a task-force that in one year resettled 130,000 refugees from Vietnam, and overall several hundred thousand Vietnamese refugees came to the U.S.

"Thanks to President Ford’s leadership," wrote Quang X. Pham, a refugee who went on to become the first Vietnamese American pilot in the Marines, "I’ve experienced America’s kindness and generosity during our darkest days."

The generosity that animated these responses has never been forgotten. Now another crisis calls. Although the U.S. has been...
the largest donor to humanitarian relief efforts, it has taken in only 1,434 Syrian. This is a dereliction.

The United States should pledge to take in 100,000 Syrian refugees in 2016. This is well within our capacity, and it is a fraction of previous resettlement efforts. To get this done, President Obama should raise the annual ceiling of refugee admissions from 70,000 to 200,000, which would include the 100,000 Syrian refugees. At the same time, the U.S. should continue to lead on aid by increasing humanitarian and development assistance to the region.

Taking these steps would enhance U.S. credibility in pressing other countries to both take in more refugees and meet the UN humanitarian appeal for funding. It would also help U.S. advocacy for the protection of refugees in Syria’s bordering states, which continue to bear the brunt of the crisis. It is critical that these countries do not arbitrarily detain refugees or return them to danger and that they allow them to work and go to school. American pleas to other nations to treat refugees humanely will have greater moral force if the U.S. leads by example.

As is often the case, a moral imperative is also a strategic one. The fate of the Syrian diaspora will have a profound effect on the world. Unless the United States, its European allies, and other wealthy nations change the current course, a generation of Syrian children will grow up poor, uneducated, and alienated. That is a recipe for instability.

We can change that future. At stake is not only the fate of hundreds of thousands of Aylan Kurdi, but the integrity of our commitment to the ideals of human dignity.