CONFERENCE MATERIAL

DAY ONE

SPONSORED BY:

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON LAW AND 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 29—NOVEMBER 30, 2012

RITZ-CARLTON HOTEL
SALONS I AND II
1150 22ND STREET, NW
WASHINGTON, DC
## Conference Material: Day One

### Panel I

**Role of the Courts in National Security Law: Past, Present and Future**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The United States Supreme Court: The Cult of the Robe in the National Security Enterprise—Harvey Rishikof</td>
<td>1</td>
</tr>
<tr>
<td>After Deference: Formalizing the Judicial Power for Foreign Relations Law—Deborah N. Pearlstein</td>
<td>21</td>
</tr>
<tr>
<td>National Security Fact Deference—Robert M. Chesney</td>
<td>75</td>
</tr>
</tbody>
</table>

### Panel II

**Intelligence Law Developments**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Development of Intelligence Law—W. George Jameson and Robert S. Litt</td>
<td>151</td>
</tr>
<tr>
<td>Speech by W. George Jameson—Safeguarding National Security Information: Dealing with Unauthorized Disclosures of Classified Information</td>
<td>167</td>
</tr>
<tr>
<td>Remarks by CIA General Counsel Stephen Preston at Harvard Law School</td>
<td>173</td>
</tr>
<tr>
<td>Intelligence Community Directive Number 122—Office of the Director of National Intelligence</td>
<td>177</td>
</tr>
<tr>
<td>Executive Order 13462 February 29, 2008</td>
<td>183</td>
</tr>
<tr>
<td>Directive Number 5143.01 November 23, 2005—U.S. Department of Defense</td>
<td>189</td>
</tr>
<tr>
<td>Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security</td>
<td>201</td>
</tr>
<tr>
<td>Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity</td>
<td>223</td>
</tr>
<tr>
<td>Memorandum of Agreement between the Secretary of Defense and the Director of National Intelligence</td>
<td>229</td>
</tr>
<tr>
<td>Remarks by Harold Hongju Koh—International Law in Cyberspace</td>
<td>231</td>
</tr>
<tr>
<td>Department of Defense Strategy for Operating in Cyberspace—July 2011</td>
<td>235</td>
</tr>
</tbody>
</table>

### Panel III

**Merging Technologies**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Impact of Technology on National Security Law—Angeline Chen and Clark Walton</td>
<td>251</td>
</tr>
<tr>
<td>Selected Articles (The Washington Post)—Robert O'Harrow, Jr.</td>
<td>271</td>
</tr>
<tr>
<td>Keeping Watch on the Detectives—David Cole</td>
<td>307</td>
</tr>
<tr>
<td>Virtual Checkpoints and Cyber-Terry Stops: Digital Scans to Protect the Nation's Critical Infrastructure and Key Resources—Scott J. Glick</td>
<td>311</td>
</tr>
<tr>
<td>Reflections on Technology and Intelligence Systems—Michael Warner</td>
<td>337</td>
</tr>
<tr>
<td>Domestic Use of Aerial Drones by Law Enforcement Likely to Prompt Privacy Debate—Peter Finn</td>
<td>383</td>
</tr>
<tr>
<td>Excerpt: Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age—Laura K. Donohue</td>
<td>389</td>
</tr>
</tbody>
</table>
Panel I:

Role of the Courts in National Security Law: Past, Present and Future

Moderator:
William C. Banks
*784 Introduction

How much deference should courts afford the executive's interpretations of statutes and treaties in foreign relations law? This question that has long engaged foreign relations scholars has found new salience in recent years, as the courts have been called repeatedly to determine the meaning of statutes and treaties bearing on the President's detention and trial powers in combating international terrorism. Among courts noting the confusion on this issue are those now attempting to address whether and to what extent the executive's views are relevant in interpreting the Authorization for Use of Military Force (AUMF), the statute the President invokes to justify continued detention of terrorist suspects at the U.S. Naval Base at Guantanamo Bay. [FN1] While the Supreme Court has offered some guidance on the scope of the statute, [FN2] the AUMF itself is silent on the question of detention. As the courts have struggled to choose between two interpretations of the statute—one put forward by the executive, the other advanced by detainees—courts have been notably equivocal on the potentially dispositive issue of judicial deference: "The Court does not accept the government's position [on the meaning of the statute] in full, then, even given the deference accorded to the Executive in this realm, because it is ultimately the province of the courts to say 'what the law is' . . . ." [FN3]

*785 Historically, most scholars have accepted with little question the notion that the Court will defer to executive views in core matters of foreign relations, particularly where matters of national security are concerned. [FN4] Yet on descriptive and normative grounds, the events of the past decade have called the prevailing account into question. In treaty interpretation, the Court has invoked a Marbury-based insistence on asserting its own formal interpretive authority. As the Court put it perhaps most dramatically in recent opinions construing the Vienna Convention on Consular Relations: "If treaties are to be given effect as federal law under our legal system, determining their meaning as a matter of federal law 'is emphatically the province and duty of the judicial department,' headed by the 'one supreme Court' established by the Constitution." [FN5] Likewise, in a series of decisions involving national security, the Court has been anything but deferential to the executive's interpretation of the relevant statute or treaty. In Rasul v. Bush, [FN6] Hamdi v. Rumsfeld, [FN7] Hamdan v. Rumsfeld, [FN8] and Bounmediene v. Bush, [FN9] the Court has swept aside vigorous arguments by the executive that it refrain from engagement on abstention or political question grounds. Moreover, the Court has scarcely noted any doctrinal tradition of interpretive "deference"*786 on the meaning of the laws. While descriptive claims that the Court invariably defers to the President in foreign relations law interpretation have always been subject to challenge, the Court's recent behavior has made this account increasingly untenable. [FN10]

In the wake of such decisions, scholars have turned renewed attention to the task of identifying a doctrine of "deference" in foreign relations law. Cass Sunstein and Eric Posner, among others, have expressed the normative concern that the Court, unduly interested in "saying what the law is" in an area of questionable judicial competence, was no longer taking sufficient account of the executive's superior expertise and political responsiveness in this realm. [FN11] Others, while not necessarily lamenting the less deferential judicial role, have focused on the importance of finding some constraining approach that would provide interpretive guidance to the courts. [FN12] If there is no predictable or sensible
way of determining how much attention the Court will pay executive views in construing foreign relations law, rule-of-law interests require, at a minimum, the development of a new understanding of the judicial relationship to the executive on questions of law interpretation. Responding to such concerns, Sunstein and Posner thus joined Curtis Bradley and others in suggesting that courts should defer to the executive in cases with “substantial foreign relations implications,” just as they do under Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc. [FN13] in the standard administrative law context. [FN14]

But as this Article contends, Chevron’s promise of resolving the deference question in foreign relations law is almost certainly overstated. *787 First, Chevron is not nearly as doctrinally stable as its advocates suggest. As a growing set of empirical studies has shown, Chevron has exerted anything but a defining hold on Supreme Court treatment of agency interpretation of federal laws. This Article will describe how the contemporary Court has regularly avoided applying traditional Chevron deference in what might otherwise have been thought to be circumstances described by the core of that doctrine. Indeed, the Court has ignored Chevron as a useful interpretive guide in recent foreign relations cases in which it might most readily be implicated. [FN15] At the same time, while one of the most important functional rationales for embracing Chevron in the foreign relations context is said to be the doctrine’s ability to take account of the executive’s superior expertise, Chevron is, in key respects, a blunt tool for ensuring that expertise is taken into account in law interpretation. An agency administrator in principle enjoys deference under Chevron whether or not the administrator has actually included the relevant agency experts in the analysis. If one accepts the view that the executive’s key strength is its expertise on certain questions arising in foreign relations, one would presumably wish to insist that the actual experts inside the executive branch be consulted. If expertise matters, there may be more effective ways of ensuring its inclusion than review for generalized “reasonableness” of “executive” interpretation.

Beyond this, the wholesale importation of Chevron into foreign relations law poses another problem. As Chevron’s critics have emphasized since soon after the decision came down, Chevron appears to be in tension with the Court’s formal constitutional power under Article III, which has at its core the duty to “say what the law is.” [FN16] When the Court does something less than determine for itself what the law is, the argument goes, it is ceding power that the Framers of the Constitution intended to reserve to the Article III courts. [FN17] While administrative law scholars have grappled with this problem for decades, it has been surprisingly absent from the contemporary foreign relations law debate. Yet importing Chevron into the foreign relations setting without attempting to address the issue only perpetuates the formal dilemma. Particularly because the formal allocation of foreign relations power between the judicial and executive branches—unlike the rather more novel authority of administrative agencies—is an express subject *788 of constitutional concern, it seems essential to have some formal theory of how interpretive power may be shared in this realm before designing a deference doctrine that effectively shares it. At what point does a preemption of the judicial interpretive inquiry—in favor of the executive’s meaning—chip away at a formal authority the Constitution otherwise grants to the courts? Once a “case or controversy” is properly before an Article III court, is there a formal floor of judicial power to interpret statutes and treaties, beneath which no functional deference rationale can justify allowing the court to sink? Without some more developed understanding of what is meant by the “judicial power” in foreign relations law, it is premature to settle on a deference regime that may have the court adjusting its approach to law interpretation. This Article begins exploring answers to these questions of formal power.

Part I engages the current debate over judicial deference in foreign relations interpretation. While embracing the need for greater clarity, it argues that importing Chevron into foreign relations law is an unsatisfying solution. Part II then takes up the problem of formal judicial power in detail, considering first the two leading accounts of the “judicial power” in statutory interpretation. The first model, still perhaps the dominant understanding of the courts’ role in statutory interpretation, known as “faithful agent” theory, sees the relationship between Congress and the courts as that of principal and agent, where the judicial agent’s duty is limited to attempting to discern and accurately apply the directions
of the legislative principal set forth in statute. [FN18] Yet as will be discussed, faithful agent theory seems unlikely to fully explain the judicial role in foreign relations law. In statutory interpretation, it is not immediately clear that it leaves room for an executive interpretive role of any sort. For treaty interpretation, faithful agent theory's utility is even more suspect. Treaties, of course, are not concluded by the legislature alone, but are "made" by the executive, "by and with the advice and consent of the Senate." [FN19] Indeed, the U.S. executive and Senate are not the sole lawmakers involved in making treaties; foreign treaty partners help conceive, negotiate, and draft the legal text. [FN20] In this context, *789 it seems problematic at best to view the U.S. executive as the sole "principal" lawmaker whose intent the Court must discern.

A second model of the judicial power, commonly called "instrumental theory," is somewhat more promising. It holds that Article III courts were created not to be mere agents of Congress, but rather to employ quintessentially judicial canons of interpretation and methods of legal reasoning that will both help to clarify ambiguous texts and influence legislative drafting over time. [FN21] Yet while instrumental theory adds much value to the question of judicial power in foreign relations law, it too leaves central questions about the relationship between the interpretive power of the courts and the executive unanswered. Instrumental theory's relative silence on the role of normative canons of statutory construction [FN22]—for example, an avoidance canon that requires a clear statement before rendering an interpretation that has the effect of delegating power from one branch to another—leaves unsettled one of the central questions in foreign relations law: whether interpretive canons of constitutional stature still apply. [FN23] Likewise, it seems hard to believe that the judicial power in treaty interpretation hinges on the expectation that interpretive practices pursued by the U.S. judiciary alone are meant to have a clear impact on treaty drafting over time. While the U.S. executive certainly has some incentive to take Supreme Court interpretive expectations into account in negotiating treaty texts, the United States' system is but one judicial system among many in multilateral treaty interpretation. Foreign courts are hardly bound by the interpretive guidance of the U.S. high court, and our treaty partners may have their own domestic interpretive demands to fulfill. Under the circumstances, it would seem *790 surprising if instrumental influence of this sort were the sole, or even primary, expected judicial function in treaty interpretation.

Given these deficiencies, this Article turns in Part III to offer a separate, supplemental understanding of the judicial power in foreign relations law. Here called equilibrium theory, the model this Article explores draws on historic justifications for judicial supremacy over constitutional interpretation to propose that part of the judicial role in statutory and treaty interpretation is to aid in maintaining a structural balance of power. [FN24] As Monaghan has noted, "Marshall's grand conception of judicial autonomy in law declaration was not in terms or in logic limited to constitutional interpretation." [FN25] And while the most sweeping conceptions of judicial power to independently "say what the law is" [FN26] could not survive the modern administrative state, it is a mistake to understand this transformation as the end of the Court's role in structural power balancing. The Framers' vision of separated branches, as post-Chevron critics have suggested, was of a government of shared authority, each branch with enough constitutional power "to resist encroachments of the others." [FN27] Serving the demands of functional effectiveness by allowing one branch to accrue greater authority over time may be permissible as long as the other branches can respond with equal and opposite constraining force of their own. Delegation could be tolerated, but only because it was possible to maintain an offsetting power through judicial review. [FN28] In this view, to the extent a doctrine of deference disables the courts from helping to maintain that system of "dynamic equilibrium," [FN29] it impermissibly encroaches on the structural mandate of the judicial power.

Such an understanding of the judicial power contributes to our approach to deference in statutory and treaty interpretation in several ways. First, there is nothing in equilibrium theory that would preclude the consideration of an executive branch interpretation of a law, particularly insofar as the executive may enjoy functional advantages in expertise that might clarify legislative meaning, or insofar as the executive *791 has a relevant formal role (i.e., to "make" treaties). There would, however, be an expectation in statutory interpretation that the Court would apply substantive interpretive
canons geared toward limiting excessive delegations of power and disfavor interpretations that disable any one branch from continued participation in a deliberative dialogue. And there would be a corresponding expectation in treaty interpretation—an expectation that domestic judicial power would function, at least at the interpretive margins, to push back against the tendency in international law and legal structures to aggrandize power for executives within domestic legal systems. [FN30] As a result, an equilibrium theory understanding of the limits of judicial deference has direct implications for the interpretation of statutes like the AUMF, a statute whose meaning is informed by international law and so occupies the courts today. [FN31]

Before proceeding, it may be helpful to say a word about what the field “foreign relations law” is meant here to describe. The term itself may be most commonly read to capture a set of cases involving disputes or other engagements between the United States and other nations. Cases involving treaty interpretation thus seem centrally implicated. At the same time, most scholars in the field recognize that certain questions of statutory interpretation might also fall within the “foreign relations” rubric—particularly statutes implicating special functional strengths of the executive branch and statutes seeming to implicate the executive’s own formal constitutional role. [FN32] Given both the potential breadth and the uncertain stability of such a category, a deference doctrine intended for the (said) peculiar demands of foreign relations law might easily become the exception that swallows the rule. Be that as it may, it nonetheless seems worthwhile to consider whether it is possible to identify a theory of judicial power that would help inform the Court’s approach to executive views across this admittedly broad range of cases.

The justifications for this approach are multiple. First, the text of Article III setting forth the formal judicial power itself does not distinguish*792 between statutes and treaties: “The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made . . . .” [FN33] That is, the same judicial power appears to extend to any of the subject instruments. It may be the case that formal power granted to the executive (in foreign relations but not elsewhere) has some effect on what deference the courts owe, and this Article will consider arguments supporting this possibility. But because in the first instance the inquiry here is about the scope of the judicial power since Marbury, it seems necessary to begin by asking about the judicial power in general.

Second, however unstable the category of “foreign relations law” may be, it is a field that both courts and scholars have long recognized as having some exceptional salience in informing how the Court should behave. By embracing the full breadth of the category—including its extension to both statutes and treaties—we might better understand how exceptional the category really is. If foreign relations law is indeed increasingly indistinguishable from ordinary domestic law—either in its formal attributes (e.g., texts, history, and decisional law) or in the functional skills its application demands (e.g., expertise and political accountability)—that is all the more reason to ensure that any doctrine of “deference” in the field flows from some common understanding of the judicial role.

I. The Problem of Interpretation in Foreign Relations Law

Scholars have long posited that the courts defer to executive views in interpreting foreign relations law, particularly where matters of national security are concerned. [FN34] In statutory interpretation, the Court has broadly construed legislative delegations of power to the President. [FN35] Deference is all the more evident in treaty interpretation, it is argued, where the President’s record of prevailing in the Supreme Court is lengthy [FN36] and where the President’s power to *793 “make treaties” may give the Court formal reasons to accede to the President’s interpretive wishes. [FN37] Counternarratives exist, to be sure, but they have had seemingly modest effect in puncturing the prevailing wisdom. [FN38] Yet on descriptive and normative grounds, the Court’s behavior in the past decade especially has called the prevailing account into question. This Part thus begins by highlighting some of the Court’s recent decisions that have posed the
greatest challenge to historical expectations of deference in foreign relations law. It then considers whether recent proposals to address the muddle of deference doctrine in foreign relations law succeed in remedying the problems their proponents hope to address.

A. Foreign Relations Deference in the Modern Court

The notion that the Court defers regularly to the executive’s views in foreign relations law manifests itself somewhat differently in doctrines of treaty and statutory interpretation. In treaty interpretation, the strongest argument that the Court defers to the executive’s reading comes from a small number of twentieth-century cases in which the Court has noted that the “meaning given [treaties] by the departments of government particularly charged with their negotiation and enforcement is given great weight.” [FN39] To be clear, this “great *794 weight” language is invariably qualified immediately before or after by insistence that the executive’s views are in no way “conclusive” on questions of interpretation. [FN40] Indeed, most treaty cases that find the Court commenting at all about its interpretive methodology begin with familiar textualist statements to the effect that “[i]n construing a treaty, as in construing a statute, we first look to its terms to determine its meaning.” [FN41] A fair number of Supreme Court treaty cases say nothing at all about notions of interpretive deference to the executive. [FN42] Nonetheless, Curtis Bradley, among others, has argued that such language “is not mere window dressing, but rather is a significant factor in treaty interpretation.” [FN43] And while raw outcome statistics tell us little about the role of deference doctrine as a dispositive factor in Supreme Court treaty interpretation, the executive has succeeded in winning far more treaty interpretation cases than it has lost. [FN44]

In statutory interpretation, strong notions of judicial deference to the executive in foreign relations matters are traced most commonly to United States v. Curtiss-Wright Export Corp., a non-wartime case in which the Court embraced the President’s reading of a statute delegating authority to the executive to place an embargo on arms sales to certain countries. [FN45] Rejecting a nondelegation challenge to the President’s exercise of authority, the Court wrote sweepingly of “the very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations,” [FN46] a “vast external realm” [FN47] in which “the President alone has the power to speak or listen as a representative of the nation.” [FN48] Without making clear the full consequences of this description for statutory interpretation, Curtiss-Wright has been understood to suggest that standard canons of interpretation (in particular, construing the text against instituting overly broad delegations of power) are less salient in matters of *795 foreign relations. [FN49] While Curtiss-Wright has been the subject of scathing criticism over the years, [FN50] it is broadly thought to contemplate exceedingly deferential attention to the President’s construction of statutory grants of authority. [FN51]

Whether or not deference doctrines in treaty and statutory interpretation have ever had much stability or influence, [FN52] they have been little in evidence in the Court’s interpretive methodology in recent years. This Section highlights some of the more important opinions in this regard, concluding that the Court has shown no inclination to preterm its own interpretive inquiry so that it might defer to an interpretation advanced by the executive. On the contrary, these cases are most readily understood to embrace the vigorous assertion of the Court’s own formal power of interpretation, including the wide-ranging consideration of functional arguments advanced by all sides.

*796 1. Interpreting Treaties

Perhaps the most instructive set of cases from the modern Court illuminating treaty interpretation has been the series addressing the domestic effect of Article 36 of the Vienna Convention on Consular Relations, [FN53] which requires authorities to inform a noncitizen arrestee of her right to notify her home consulate of an arrest or pending prosecution in U.S. courts. [FN54] In Breard v. Greene, the Court held that state procedural rules requiring defendants to raise treaty
claims at trial or waive those claims on appeal could prevent a defendant from having the claim heard at all in a subsequent federal habeas proceeding. [FN55] But soon after the Breard decision came down, the International Court of Justice (ICJ)—which an optional protocol to the Convention named as having "compulsory jurisdiction" over "[d]ispute[s] arising out of the interpretation or application of the Convention" [FN56]—ruled to the contrary. According to the ICJ, the application of a state procedural default rule to block habeas consideration of a defendant's treaty claim violated Article 36 of the Convention because it "had the effect of preventing 'full effect [from being] given to the purposes for which the rights accorded under this article are intended.'" [FN57]

The Supreme Court took up the effect of the ICJ ruling in two subsequent opinions—both of which seem most distinguished for their vigorous defense of the power of the Court itself. Sanchez-Llamas v. Oregon involved the failure of the Virginia state police to notify Mr. Sanchez-Llamas of his right to consular notification following his arrest. [FN58] In rejecting Sanchez-Llamas's argument that suppression of evidence was a proper remedy for an Article 36 violation, the Court made no mention of a canon of interpretive deference. [FN59] On the contrary, to the extent the Court discussed its interpretive approach, it was with simple reference to the Restatement version of treaty construction: "An international agreement is to be interpreted in good faith in accordance with the ordinary meaning to be given to its terms in their context and in the light of its object and purpose." [FN60] Likewise rejecting the suggestion that the Court must accept the ICJ's decision as authoritative on the treaty, [FN61] the Court emphasized that it could not be bound by the judgment of another judicial body. [FN62] The Court's reasoning on this point did not begin with any discussion of deference (to the executive's views or those of anyone else), but instead with a ringing endorsement of the power of the independent judiciary: "If treaties are to be given effect as federal law under our legal system, determining their meaning as a matter of federal law 'is emphatically the province and duty of the judicial department,' headed by the 'one supreme Court' established by the Constitution." [FN63] Only after concluding, based on its own reading of the ICJ's enabling statute, that "[n]othing in the structure or purpose of the ICJ suggests that its interpretations were intended to be conclusive on our courts," did the Court note in its final paragraph that the interpretations of "the departments of government particularly charged with [treaties'] negotiation and enforcement is given great weight." [FN64] As it turned out, the Court said, the executive agreed with its judgment that ICJ rulings are not binding on U.S. courts. [FN65]

Yet even this passing notice of deference to the executive ultimately rang hollow. In 2005, the year before Sanchez-Llamas, President Bush issued a memorandum opinion stating that the United States would discharge its international obligations under the ICJ judgment by "having State courts give effect to the [ICJ] decision in accordance with general principles of comity in cases filed by the 51 Mexican nationals addressed in that decision." [FN66] If the Sanchez-Llamas Court had been principally interested in giving effect to the President's desired outcome in these cases, one might imagine it would have been at least possible to construe the relevant texts to require that state courts give the decision such an effect. Instead, the Court went to great lengths to restate the executive's more nuanced position on the Court's own terms. While the executive had "agreed to 'discharge its international obligations' in having state courts give effect to the [ICJ's] decision," it did not expressly take the position that the ICJ's interpretation binds U.S. courts. [FN67]

In this light, the Court's more recent decision in Medellin v. Texas [FN68] was of a piece with its equivocal response to the executive's views. Asked to determine whether the ICJ's judgment itself gave petitioners an enforceable right, the Court began with the same familiar, non-deferential statement of treaty interpretation. [FN69] While the Court agreed with the executive that the relevant treaties did not render ICJ decisions directly enforceable in U.S. courts, it was only after the Court thoroughly considered and rejected Medellin's argument that it mentioned that "the United States' interpretation of a treaty 'is entitled to great weight.'" [FN70] Of greater significance, in rejecting the notion that the President's 2005 memorandum telling state courts to give effect to the ICJ decision required those courts to comply, the Court dismissed the executive's argument that the ICJ judgment "became the law of the land [binding on courts] pursuant to the President's*799 Memorandum and his power 'to establish binding rules of decision that preempt contrary state law.'"

Central to the executive's position on this point was that the relevant treaties should be read to "implicitly give the President" the power to implement the United States' "treaty-based obligation" to effect compliance with the ICJ's decision. [FN72] In essence, the executive was asking the Court to accept its interpretation of the treaty—a reading that would allow it to maintain that the treaty could not be enforced by courts upon the request of an individual asserting a right, but could be (indeed must be) enforced when the executive issued an informal instruction for court-based compliance. This the Court refused to do, insisting that only Congress could convert "a non-self-executing treaty into a self-executing one." [FN73] If the executive wanted to achieve this effect, it could have ensured that the treaty "contain[ed] language plainly providing for domestic enforceability." [FN74] As the Court had just concluded that the treaty could not be read that way—as one might have thought a more deferential analysis would require—the executive could not prevail.

The foregoing is hardly meant to argue that the executive's understanding of treaties is irrelevant to judicial interpretation. On the contrary, the Court clearly counts among its interpretive tools positions the executive has taken in negotiating treaties and in implementing them. [FN75] But drawing on executive views as probative of "legislative" intent (because it is reflective of the negotiating history) or as evidence of post-ratification performance is notably different from attending to the executive's views because of some functional interest in the executive's superior political accountability or expertise, as Chevron contemplates. [FN76] Because they reflect executive behavior and not a particular executive's particular interpretive views, a treaty's negotiating history and post-ratification practice may or may not turn out to support the position of any given executive in any given case. In treaties, as in contracts, performance has been understood to be evidence *800 of the parties' intent in creating the agreement; postcontract performance can inform the meaning of an ambiguous clause. [FN77] It is thus the behavior of both parties to a treaty that the Court has found probative as a matter of interpretation. [FN78] To the extent the Court attends to the executive's views, it regularly looks to the views of both negotiating partners as evidence of negotiating intent and of post-ratification performance. [FN79] As a unanimous Court put it:

Our role is limited to giving effect to the intent of the Treaty [sic] parties. When the parties to a treaty both agree as to the meaning of a treaty provision, and that interpretation follows from the clear treaty language, we must, absent extraordinarily strong contrary evidence, defer to that interpretation. [FN80]

In this context, the Court's lack of deference to the U.S. executive since September 11, 2001, on the interpretation of the international law of armed conflict (including the Geneva Conventions) should perhaps have been less surprising than it seemed. Consider Hamdan v. Rumsfeld, [FN81] which presented the Court with a challenge to the legality of military-commission trials then underway at Guantanamo Bay. Among other claims, Hamdan argued that the commission regime ran afoul of Common Article 3 of the Geneva Conventions, treaties requiring, inter alia, that trials be held in a "regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples." [FN82] The Court promptly rejected the executive's *801 initial argument—that the Court should abstain from deciding the issues in the case at all. [FN83] Rather, in light of "the duty which rests on the courts, in time of war as well as in time of peace, to preserve unimpaired the constitutional safeguards of civil liberty," the Court explained, "the public interest require[s] that we consider and decide those questions without any avoidable delay." [FN84] The Court was even more direct in rejecting the executive's claim that it should prevail on the merits of its argument that Geneva had no application to Hamdan's case. [FN85] With no mention of deference and calling the government's treaty interpretation simply "erroneous," the Court held that Common Article 3 applied to the armed conflict at issue. [FN86] While the Court recognized that the treaty was ambiguous in some respects, it did not hesitate in concluding that the executive's commissions did not satisfy what requirements there were. [FN87]

2. Interpreting Statutes

To the extent the Court's post-September 11 statutory cases have addressed the question of interpretive deference at
all, they likewise show little indication that the Court believes extraordinary deference is due in foreign relations law—and, indeed, often appear to apply a less deferential standard than the Court uses when construing statutory grants of authority to executive agencies in administrative law. Consider*802 Hamdi v. Rumsfeld,[FN88] in which the Court was called to determine whether the President's detention of a U.S. citizen, whom the government alleged the U.S. military seized during operations in Afghanistan, was authorized by the 2001 AUMF.[FN89] In defending its authority to detain Yaser Hamdi as an “enemy combatant,” the executive insisted that the question whether “captured enemy combatants are entitled to POW privileges under the [Third Geneva Convention] is a quintessential matter that the Constitution (not to mention the [Constitution]) leaves to the political branches and, in particular, the President.”[FN90]

While recognizing that the AUMF afforded the executive at least some statutory authority to detain Hamdi,[FN91] the plurality opinion reads as a vigorous endorsement of independent judicial review. As Justice O'Connor explained, the AUMF must be read to authorize Hamdi's detention not because an alternative reading would infringe the President's constitutional power or other separation-of-powers interests, but because, by the Justices' own reading of “longstanding law-of-war principles” [FN92] and international “agreement and practice,”[FN93] detention “to prevent a combatant's return to the battlefield is a fundamental incident of waging war.”[FN94] If in the Court's judgment, “the practical circumstances of a given conflict are entirely unlike those of the conflicts that informed the development of the law of war, that understanding *803 may unravel.”[FN95] Indeed, as Justice O'Connor then noted in rejecting the executive's view that the process provided to Hamdi was sufficient:

While we accord the greatest respect and consideration to the judgments of military authorities in matters relating to the actual prosecution of a war, and recognize that the scope of that discretion necessarily is wide, it does not infringe on the core role of the military for the courts to exercise their own time-honored and constitutionally mandated roles of reviewing and resolving claims like those presented here.[FN96]

Notably, whatever deference may be due—and it appeared not to be much—it was due not to the President in particular or the executive writ large, but to “the judgments of military authorities” who are functionally expert on the issue.

Hamdi's companion case, Rasul v. Bush,[FN97] tested the Court's authority more directly. The executive had argued that the federal courts lacked jurisdiction to consider petitions that noncitizen detainees held at Guantanamo Bay brought under the federal habeas statute.[FN98] Yet in rejecting the government's jurisdictional argument, the Court was not deterred by the notion that it should defer to the executive's interpretation of the habeas statute. According to the Court, the presumption against extraterritorial application of federal statutes that the executive invoked had no relevance where U.S. territory was at issue—and the military base at Guantanamo was, effectively, just such a place.[FN99]

*804 In any event, Hamdan v. Rumsfeld [FN100] soon dispelled whatever expectation of unquestioned deference on issues of statutory interpretation remained. In addition to its treaty arguments, the executive argued that the AUMF and the statutory Uniform Code of Military Justice (UCMJ) [FN101] should be read to extend executive authority to try Hamdan in a military commission. The use of military commissions was a “necessary” part of the “necessary and appropriate force” the AUMF authorized the President to use, and “courts are not competent to second-guess judgments of the political branches regarding the extent of force necessary to prosecute a war.”[FN102] In addition, the government argued that Article 36 of the UCMJ squarely “authorize[d] the President to establish procedures ‘for cases arising under this chapter triable in. . . military commissions.’”[FN103] Under that provision, the President was delegated broad authority to establish the rules for commission proceedings, including rules different from those generally recognized in criminal cases, whenever the President "considers" application of those rules to be not "practicable."[FN104] Deference was due the President's judgment on what counts as "practicable" by the terms of the statute itself. Here, the President had already made such a dispositive finding in his executive order, which provided that "the danger to the safety of the United States and the nature of international terrorism" made standard criminal trials impracticable.[FN105]
On its face, the executive's argument that it was entitled to some measure of deference in interpreting the AUMF and UCMJ seems squarely within the Curtiss-Wright tradition of interpreting delegations of power broadly. Alternatively, the executive might have been accorded Chevron deference, with the President in the role of an expert agency—and therefore one whose interpretation should prevail as long as it is reasonable. [FN106] Yet in an opinion that mentioned neither *805 Curtiss-Wright nor Chevron, the Court rejected the government's arguments in a technical, purely de novo analysis of the relevant UCMJ provisions. In the Court's view, the President's generalized finding about the viability of criminal trials was "insufficient." [FN107] Statutory language requiring commission and court martial procedures to be "uniform" to the extent "practicable" [FN108] did not say that uniformity could be waived whenever the President "consider[ed]" it impracticable. [FN109] This statutory standard required uniformity "insofar as practicable" [FN110]—a seemingly more objective test. And even if it were possible to satisfy the requirement without an "official determination," the Court deemed the impracticability requirement "not satisfied here." [FN111] Why? "Nothing in the record before us demonstrates that it would be impracticable to apply court-martial rules in this case." [FN112] Even assuming that the President's generalized finding that criminal trials were inadequate was relevant to the impracticability inquiry, and even assuming that such a finding "would be entitled to a measure of deference" [FN113] under the statute, "the only reason offered in support of that determination is the danger posed by international terrorism." [FN114] While the Court emphasized that it did not "for one moment underestimat[e] that danger," it found no specific reason in the record for challenging the notion that standard court-martial rules would work. [FN115]

The Court's most recent cases involving the availability of statutory remedies for military detainees did not substantially alter the notably nondeferential Hamdan landscape in this regard. Boumediene v. Bush struck down a key provision of the Military Commissions Act of 2006 (MCA)—one attempting to strip the courts of jurisdiction to hear the habeas petitions of Guantanamo detainees—as an unconstitutional suspension of the writ of habeas corpus. [FN116] Rejecting the executive's proposed construction of the statute that might have rendered alternative statutory procedures a constitutionally adequate substitute for habeas, the Court found the MCA constitutionally deficient despite the availability of both the canon of constitutional avoidance (which *806 the Court mentioned explicitly) and the possibility of judicial deference to executive interpretation that might have facilitated a decision finding a constitutionally permissible construction of the MCA. [FN117] While dicta in the Court's opinion indicated some deference to the judgment of the political branches that Hamdi, Rasul, and Hamdan had entirely ignored, that passing language seemed to do little work in the Court's analysis, and it did not affect the outcome of the case. [FN118]

Munaf v. Geren, [FN119] in contrast, does appear to rely on the notion of deference to the political branches. There, the Court rejected on the merits habeas petitions filed by U.S. citizens held by U.S.-led multinational forces in Iraq. Petitioners had asked the Court to enjoin their transfer to Iraqi authorities for prosecution, arguing that transfer would violate U.S. treaty and statutory obligations not to send individuals to another country where they were likely to face torture. [FN120] While *807 again rejecting the executive's contention that the habeas statute did not authorize federal court jurisdiction in the case, the Court concluded rather broadly that "in the present context [the risk of torture] is to be addressed by the political branches, not the judiciary." [FN121] Here, the State Department had determined that the Iraqi prisons have "generally met internationally accepted standards for basic prisoner needs," [FN122] and according to the Solicitor General, "the United States would object to [the multinational forces'] transfer of [petitioner] to Iraqi custody if it thought that he would likely be tortured." [FN123] The per curiam opinion embraced the executive's position, noting that the Court was "not suited to second-guess" the government's judgment of "whether there is a serious prospect of torture at the hands of an ally." [FN124]

Although the Court's attitude toward the executive here feels different, it would be a mistake to conclude that the Court's broad language has any bearing on its view of the significance of executive statutory (or treaty) interpretation. Importantly, the Court declined to reach the full merits of the detainees' statutory claims on the ground that they
had not successfully raised them in the courts below. Similarly, the deference the Court appears to be exercising is not to an interpretation by the executive of its own legal authority, but rather to its assessment of the relevant facts—namely, whether the detainees were likely to face torture at the hands of the Iraqis. Deference to an executive's finding of facts carries far less significance for our understanding of judicial power than does deference on questions of law. Appeals courts defer to superior factfinders with regularity—whether juries, trial courts, or administrative judges—with no special significance for the scope of Article III power. With Munaf most easily read to embrace this brand of deference, it has fewer implications for the power of the courts "to say what the law is." [FN125]

B. The Elusive Promise of Chevron

In the wake of such decisions, it is not surprising that scholars have turned renewed attention to the task of identifying a doctrine of "deference" in foreign relations law. Whether driven by the normative*808 concern that the Court was no longer taking sufficient account of the executive's superior expertise and political responsiveness, [FN126] or by the rule-of-law interest in providing some interpretive guidance to the Court, [FN127] the particular challenge of balancing the executive's interpretive power against the Court's has reemerged as a vexing problem. While rejecting the notion that the executive's "privacy in the interpretation of international law" gives him the power to ignore treaty requirements that are otherwise clear, scholars such as Sunstein and Posner have argued that courts should defer to executive interpretations of ambiguous statutes and treaties in this realm. In much the same way deference has been given to executive agency interpretations since the Court's watershed opinion in Chevron. [FN128] Chevron famously established a two-step inquiry that courts were to follow in ascertaining how to account for executive views when reviewing agency interpretations of statutory authority. Where the Court finds statutory meaning clear in the first instance, no further interpretive inquiry is necessary. [FN129] But where the meaning of the statute is ambiguous, the Court ceases its usual exercise in determining the law's import and inquires only whether the executive agency's interpretation is a "permissible construction of the statute." [FN130] If it is, no further judicial inquiry into the meaning of the law is necessary. So too, Sunstein and Posner have suggested that, in foreign relations law, the executive's interpretation of ambiguous laws should prevail as long as its interpretation is reasonable. [FN131]

In this view, Chevron is thought to carry several advantages over a more generalized assumption of judicial deference to the President in the foreign relations setting. Chevron is "well-entrenched in the Supreme Court, with all of the nine current justices [at the time of *809 Bradley's writing] accepting its basic framework." [FN132] It thus promises a more regularized approach to judicial engagement with executive law interpretation and could help not only cabin judicial discretion, but also clarify the rules of interpretation for Congress, agencies, and lower courts. [FN133] Moreover, Chevron could serve an important set of functional goals:

[Chevron] pushes "interpretive lawmaker" to government entities that have more expertise and democratic accountability than courts. In addition, by centralizing this lawmakers in the executive branch rather than in a diffuse court system, the Chevron doctrine is designed to promote uniformity in the law. And by allowing for changes in interpretation, it seeks to promote flexibility in regulatory governance. [FN134]

It is argued that, if anything, the doctrine's functional rationale—grounded in the executive's superior political accountability and expertise—is even stronger in foreign relations than in traditional administrative law. Because the executive bears the primary political burden of failures in foreign relations, the executive attends to those relationships closely and is best positioned both to assess present facts and to predict what future consequences legal interpretations will have. [FN135] Chevron thus offers a useful middle ground between the near-total deference courts were thought to have shown in foreign relations law, and a Marbury-based insistence that the Court's approach to statutory and treaty interpretation should be fundamentally independent of executive views.
In exploring methods of guiding judicial engagement with executive views, there can be little doubt that the Court's recent foreign relations cases challenge traditional accounts of judicial deference. Yet the perceived strengths of Chevron in particular—in doctrinal clarity and attention to functional concerns—may be more elusive than its advocates suggest. Chevron's doctrinal stability is in fact increasingly precarious, and its flexibility in taking functional interests into account is in key respects quite limited. More than that, Chevron carried with it, and still carries, substantial questions about how it may be applied while maintaining*810 the integrity of the formal judicial power. In the years after Chevron came down, many scholars saw the decision as a sign that the Court was prepared to abdicate a significant portion of the judicial power identified in Marbury "to say what the law is." [FN136] It was one thing for a court to take executive fact-finding and expert analysis into account in understanding the scope of Congress's delegation. It was another thing for the Court to preterm its own interpretive inquiry because the executive had a greater claim to democratic legitimacy across the board. If the executive's political bona fides matter in interpreting laws delegating power to an agency, why not cede interpretive power to the executive altogether? While scholars have developed a set of theories attempting to explain how the judicial power may be shared in this regard, as shall be discussed below, the formal dilemma very much persists. For these reasons, as this Section details, Chevron seems a less than ideal candidate for resolving how the courts and the executive should share interpretive power in the law of foreign relations.

1. The Chevron that Survives

It is perhaps more than a little ironic that Chevron has gained interest from foreign relations scholars at the same time that scholars of administrative law have been demonstrating with increasing persuasiveness how limited the impact of Chevron has been in cases reviewing agency statutory interpretation. One of the most comprehensive empirical studies available finds that, from the time Chevron was decided in 1984 through the Court's 2003 Term, Chevron "was applied in only 8.4% of Supreme Court cases evaluating agency statutory interpretations." [FN137] Indeed, to the extent it is possible to tell a unified, qualitative story about the trajectory of the Court's major administrative law cases since 1984, it is mostly a story that sees the Court narrowing the range of agency decisions to which Chevron might apply and insisting upon the significant interpretive power the Court retains even within the Chevron regime. More, it shows a Court chafing against the sometimes*811 awkward limits Chevron seems to impose on why executive views might matter and when they may be taken into interpretive account.

The story of Chevron's less-than-transformative impact is not inconsistent with the doctrine's origin and history. By the time Chevron came down in 1984, the Court had been grappling for decades with how to treat executive agency interpretations of federal statutes. [FN138] In this effort, the Court had long recognized—as it reiterated in Chevron—that executive agency views could help give a "full understanding of the force of the statutory policy" when a given situation "depend[s] upon more than ordinary knowledge respecting the matters subjected to agency regulations." [FN139] Nonetheless, as Chevron itself insisted, "[t]he judiciary is the final authority on issues of statutory construction and must reject administrative constructions which are contrary to clear congressional intent." [FN140] Judges were to retain significant independent authority to determine whether a statute is clear or ambiguous—often the end of an interpretive inquiry—and to determine whether an agency's interpretation is "reasonable," also a seemingly broad retention of power. [FN141]

Nonetheless, Chevron was broadly seen as revolutionary in identifying the executive's superior political accountability—and the Court's correspondingly limited credentials in that realm—and in citing that functional strength as a central basis for deferring to an agency interpretation of a statute. [FN142] As the Court famously explained: "While *812 agencies are not directly accountable to the people, the Chief Executive is, and it is entirely appropriate for this political branch of the Government to make such policy choices" in interpreting ambiguous statutes. [FN143] Accordingly, "federal judges—who have no constituency—have a duty to respect legitimate policy choices made by those who do."

[FN144] Statutory interpretation was, at least at the ambiguous margins, a task that demanded policy judgments of various sorts—judgments best carried out by one or the other political branch. It would thus be assumed that an ambiguous statute was Congress’s implicit attempt to leave some interpretive power with the executive agency.

Yet the Chevron-revolution understanding quickly bumped up against a series of indications from the Court that the case was perhaps intended as a less dramatic shift than it first appeared. Just two terms later, the Court clarified Chevron’s import in this respect. In INS v. Cardoza-Fonseca, [FN145] the Court rejected a statutory interpretation offered by the federal Board of Immigration Appeals (BIA) and emphasized the extent to which the Court retains interpretive primacy. [FN146] It also made clear the potential frequency with which the Court could decide matters of interpretation at Chevron’s first step:

The judiciary is the final authority on issues of statutory construction and must reject administrative constructions which are contrary to clear congressional intent. If a court, employing traditional tools of statutory construction, ascertains that Congress had an intention on the precise question at issue, that intention is the law and must be given effect. [FN147]

If, as in Cardoza-Fonseca, the statute’s text and ordinary canons of construction persuade the Court that the statute is clear, the agency’s view is irrelevant. Justice Scalia wrote separately, insisting that the Court’s purported clarification was in fact an “evisceration of Chevron.” [FN148] If the Court is able to ignore an agency’s statutory interpretation any time the Court thinks it can glean the meaning of the statute on its own, Chevron is no more than a “doctrine of desperation.” [FN149] As *813 it turned out, Justice Scalia was hardly alone in assessing the case as a challenge to the revolutionary view of Chevron. [FN150]

The years since Cardoza-Fonseca have seen the development of a line of decisions that further limit the range of cases in which Chevron guides judicial engagement with agency interpretation. [FN151] United States v. Mead Corp., for instance, presented the question of whether a tariff classification ruling by the U.S. Customs Service was entitled to Chevron deference. [FN152] The Court held that it was not. [FN153] In the Court’s view, there was no indication in the agency’s ruling letter that the agency “ever set out with a lawmaking pretense in mind when it undertook to make classifications like these.” [FN154] Mead thus clarified the existence of what scholars have since called Chevron step zero. [FN155] That is, before the Court considers whether a statute is ambiguous, it must determine (not just assume) that Congress intended to delegate the agency the power to issue rules with the force of law and that the agency interpretation to which deference is claimed was in fact promulgated in the exercise of that power. [FN156] In the absence of such an express delegation of legislative power, Chevron does not apply. Instead, the Court would employ the more flexible, pre-Chemene doctrine of attention to executive views outlined in Skidmore v. Swift & Co. [FN157]—that agency views are entitled to respect “to the extent that those interpretations have the ‘power to persuade.’” [FN158] As the Mead Court put it, “The *814 fair measure of deference to an agency administering its own statute has been understood to vary with circumstances, and courts have looked to the degree of the agency’s care, its consistency, formality, and relative expertise, and to the persuasiveness of the agency’s position.” [FN159]

At the same time, the Court has also moved to limit Chevron deference based on a new theory that seems to turn Chevron’s political-accountability rationale on its head. Consider FDA v. Brown & Williamson Tobacco Corp., [FN160] in which tobacco companies challenged the authority of the Food and Drug Administration (FDA) to issue a rule regulating tobacco as a drug (and thereby limiting its marketing to children). Rejecting the FDA’s interpretation of its own authority as extending to the regulation of tobacco products, a bare majority of the Court effectively explained its decision not to defer to the agency on the grounds that some issues were too political to be left to the more political branch. [FN161] Foreshadowing Mead, the Court explained that where the “history and the breadth of the authority that the FDA has asserted” would give it the power to ban cigarettes entirely, ending a multibillion dollar industry and the manufacture
of a product with a “unique political history” in the United States, Congress would have been much clearer than it was in expressing its intent to delegate to the agency such authority in the statute. [FN162] Given the political stakes, the Court preferred its own, highly contextual construction of the statute (ironically attributing the result to Congress) to that of the FDA—the agency’s superior political accountability notwithstanding. [FN163]

*815 The extraordinary-cases principle seems to cut to the core of what made Chevron seem so radical. If the Court’s awareness of its limited political accountability were Chevron’s primary raison d’etre, one would assume that it would be precisely in these extraordinary cases that the Court’s deference to the judgment of the political branches would be at its height. Yet however counterintuitive its rationale (at least from this perspective), the extraordinary-cases exception has now appeared more than once. Both in refusing to defer to the Attorney General’s finding that doctors assisting terminally ill patients to commit suicide pursuant to an Oregon law would be subject to prosecution under the federal Controlled Substances Act, [FN164] and in rejecting the Environmental Protection Agency’s interpretation that it lacked the statutory authority to regulate greenhouse gasses, [FN165] the Court has denied Chevron deference on the grounds that Congress could not have intended to delegate interpretive power of such political salience. As the Court put it most memorably, Congress “does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.” [FN166]

The Court’s most recent Chevron decisions have reinforced that its formal interpretive power extends even to cases tenuously falling under Chevron. These cases also appear to embrace the Skidmore-type view that what determines the weight accorded the executive’s interpretation is not merely that it comes from the executive, but that it comes from a process or with a record that renders the interpretation persuasive on its own terms. In Negusie v. Holder, for instance, the Court reviewed the Board of Immigration Appeals’s (BIA’s) interpretation of a statute that was, by the Court’s own assessment, ambiguous. [FN167] The Court thus noted at the outset that Chevron deference would apply: as long as the agency’s interpretation was reasonable, the Court would defer to the agency view. [FN168] Indeed, as Justice Kennedy wrote for the *816 majority: “Judicial deference in the immigration context is of special importance, for executive officials ‘exercise especially sensitive political functions that implicate questions of foreign relations.’” [FN169] Yet the Court then proceeded to reject the BIA’s reading of the relevant statute as a mistake in interpretation, concluding that in its case-by-case application of the statute, the agency had erroneously thought itself bound by an earlier Supreme Court case: “The BIA deemed its interpretation to be mandated by [the Court’s earlier decision in] Fedorenko, and that error prevented it from a full consideration of the statutory question here presented.” [FN170] The BIA had thus not actually exercised its interpretive authority but simply determined that Fedorenko controls.

The Court’s reasoning in Negusie is a puzzle in several respects. First, it is not at all clear what distance exists between “exercising interpretive authority” and applying law an agency believes to be binding. Applying relevant precedent would seem to be part and parcel of exercising interpretive authority. As long as agency interpretation of precedent is “reasonable,” it should receive Chevron deference. Perhaps to avoid this dilemma, Justice Kennedy’s opinion turned Chevron upside down: “Whether [the agency] interpretation would be reasonable, and thus owed Chevron deference, is a legitimate question; but it is not now before us.” [FN171] Chevron, of course, would have the Court inquire first as to whether the statute was ambiguous—a determination that it had already made in this case. Having decided that the statute was ambiguous, the Court’s only remaining inquiry under Chevron was to the reasonableness of the BIA’s interpretation. The Court did not engage in this inquiry. It therefore seems that the Court was not applying Chevron in any direct sense. Instead, the Court emphasized that, statutory ambiguity notwithstanding, the agency had not done enough to justify Skidmore deference. In remanding the case to the agency to try again to exercise its “Chevron discretion,” the Court was expressly prescriptive. It held that the agency must “bring its expertise to bear upon the matter; . . . evaluate the evidence; . . . make an initial determination; and, in doing so, it can, through informed discussion and analysis, help a court later determine whether its decision *817 exceeds the leeway that the law provides.” [FN172] In short, the agency
view was relevant not per se but only insofar as it could contribute something to the task of interpretation that the Court itself could not.

Regardless whether it is fair to say the Court has replaced Chevron with, as Justice Scalia put it, "th'ol' 'totality of the circumstances' test," [FN173] it is hard to argue that the Chevron doctrine is settled. The Court does not afford agencies deference every time an ambiguous statute is before it. The Court remains interested in, and determined to engage, a variety of functional factors in weighing the relevance and persuasiveness of executive views in a growing range of circumstances: where Congress has not delegated power to issue rules with the force of law, where the political consequences of the interpretive question are too important to leave to the broad discretion of an executive agency, and, as ever, where the Court feels capable of managing the interpretive task on its own. Political accountability matters, but so do subject-matter expertise and a reasoned decisionmaking process that takes that expertise into account. In Chevron and thereafter, the Court has asserted a strong, if incompletely theorized, sense of its own formal authority to say what the law is--both within the confines of the doctrine and without. In short, Chevron does not seem likely to serve as a panacea for interpretive confusion if imported into the realm of foreign relations law.

2. Chevron's Functional Failings

While foreign relations scholars may be overly optimistic about the ability of Chevron to bring doctrinal clarity to the allocation of interpretive authority between the Court and the executive, they are right to consider the role of functional interests, such as expertise and accountability, in assessing how the Court should engage executive interpretations of law. To the extent that sharing duties in law interpretation raises separation-of-powers concerns, functional analysis is often unavoidable—and it is sometimes required to understand the structural provisions of the Constitution. [FN174] Sunstein and Posner may be "818 faulted for paying insufficient attention to the protection of individual rights as a functional interest in separation of powers, with an equal or greater claim to structural priority than interests in accountability and expertise. [FN175] Their claims may also overstate the executive's institutional competence to handle security matters with minimal involvement of the other branches. [FN176] But Sunstein and Posner are right that functional interests in accountability and expertise are at least as salient in matters of national security and foreign relations as they are in traditional administrative law. [FN177]

It is worth pausing on this conclusion, for it runs counter to past assumptions that "[t]he propriety of deference may well vary depending on the type of law at issue." [FN178] Indeed, there are increasingly strong reasons to doubt both the prescriptive and normative validity of such subject-matter exceptionalism. The modern national security bureaucracy, like more traditional administrative settings, channels decisionmaking through a set of existing organizations and agencies, each with its own highly elaborated set of professional norms and responsibilities, standard processes, identities and culture. [FN179] At the same time, the growing set of societal challenges that are counted as a threat to "security" may swamp traditional distinctions between policy that is "foreign" and "domestic." [FN180] On functional grounds alone, it is increasingly difficult to see why the type of law per se--"foreign" or otherwise--should make the executive's attempts at law interpretation more or less worthy of deference.

But it is this seeming recognition that makes it especially puzzling that scholars such as Sunstein and Posner would embrace Chevron as a means of ensuring that the Court attends to the views of relevant experts. As Sunstein and Posner acknowledge, "[A]n agency receives Chevron deference even if the Administrator decides on a course of conduct that departs from the views of her informed staff. Courts do not look behind the agency's process to explore who, exactly, influenced the decision and to what extent." [FN181] If one accepts the view that the executive's key strength is its expertise on certain questions arising in foreign relations law, one would presumably wish to insist that the actual experts inside the executive branch be consulted. It is, as Sunstein and Posner note, the State Department—not, for example, White
House Counsel's office—that most carefully tracks U.S. relations with foreign states. [FN182] Indeed, it is in part because of Chevron's limitation in this regard that the Court has sometimes declined to apply it, even in the standard administrative law realm. The Court's decision in Massachusetts v. EPA, [FN183] for instance, reflects this view. Declining to afford Chevron deference to the agency's decision not to regulate greenhouse gas emissions, the Court emphasized the limited persuasiveness of the agency's reasoning. In particular, according to the Court, the EPA had not consulted with the State Department before taking the position "that regulating greenhouse gases might impair the President's ability *820 to negotiate with 'key developing nations' to reduce emissions." [FN184] So, too, it may have mattered to the Hamdan Court that the Judge Advocate General corps of military attorneys inside the Pentagon had not engaged (and did not support) the President's view of the necessity of military commissions. [FN185] Where expertise matters, the Court seems to recognize that there are more effective ways of ensuring its inclusion than reviewing the general "reasonableness" of "executive" views per se. [FN186]

The remaining functional reason for preferring Chevron in the foreign relations setting would be if one assumed—as Chevron originally appeared to [FN187]—that the functional value of political accountability is more important than any other functional value in allocating interpretive power, including that of expertise. But there is no clear reason to think accountability should be given functional superiority in this sense. Compared to functional interests in protecting individual rights or promoting expertise and effectiveness, political accountability has seemed a marginal concern among those functional interests identified in the Court's separation-of-powers jurisprudence, appearing in dissents more often than in majorities. [FN188] More to the point, *821 there is some reason to think that "deference" to the executive in some foreign relations settings will undermine, rather than enhance, political accountability. The notion that the executive is substantially more politically accountable than the courts may be especially questionable in the national security context. [FN189] Whereas in other realms of administrative law it may be plausible to argue that major agency decisions will enjoy "the kind of public scrutiny that is essential in any democracy," [FN190] appropriate government interests in secrecy surrounding certain aspects of national security may make it impossible for political accountability checks to function effectively. "That is, it is precisely because security sometimes requires secrecy that the involvement of more than one branch may be required to make public accountability possible at all." [FN191] Taking functional interests seriously, it is thus possible to conclude—as the Court increasingly has in traditional administrative law—that Chevron is at times too blunt an instrument for taking those interests into account.

3. The Persistent Formal Dilemma

While functional concerns understandably tend to dominate the question of judicial deference in foreign relations law, perhaps the greatest challenge to the successful importation of Chevron into foreign relations law is a formal one. Chevron's attempt to negotiate the formal sharing of interpretive power between the courts and the executive remains one of the great unsettled debates of the modern administrative state. Indeed, as Chevron's critics argued, when the Court does something less than determine for itself what the law is, it is ceding interpretive power that the Framers of the Constitution intended *822 to reserve to the Article III courts. [FN192] A large swath of administrative law scholarship since Chevron has thus been occupied with explaining how any sharing of interpretive duties is consistent with the presumed first-order allocation of interpretive authority to the Article III courts. [FN193] These theories shall be considered in detail in the Part that follows.

Despite this, most scholarship arguing in favor of interpretive deference in the foreign relations context has been little troubled by such formal concerns. This is not to suggest that there has been no acknowledgement of Marbury v. Madison and related formal conceptions of the judicial role. To the contrary, as Curtis Bradley has usefully summarized, the "Marbury perspective" has been expressed by a number of foreign relations law scholars, typically in objecting to deference on the basis of the executive's functional claims of superiority in matters of national security. [FN194] Yet while
the passing formal assertion that the judicial role is to "say what the law is" [FN195] may have been a reasonable--and reasonably stark--reply to the most expansive historical claims of executive power, [FN196] it seems an insufficient account of the role of the courts in the modern administrative state. Since Chevron in particular, the Court has, at least to some extent, shared the job of "saying what the law is," occasionally deferring to "reasonable" agency interpretations in realms of administrative law hardly limited to foreign relations. Since Hamdan especially, there can no longer be a question that the Court intends to assert its formal power in foreign relations law as well. Just as administrative law has had to confront what such deference means for the modern judicial role beyond Marbury, foreign relations law must recognize that as long as the courts retain any independent interpretive authority in reviewing statutes and *823 treaties, there must be a theory of the "judicial power"--and an associated doctrine of deference, vel non--that explains how the interpretive role may be shared.

While embracing the administrative law model in many respects, and indeed suggesting that the Court extend Chevron so that it might defer to the executive's interpretation in foreign relations cases even when the underlying law is not ambiguous, Sunstein and Posner offer only passing formal defense of their argument. To the extent that they address formal constraints, Sunstein and Posner note that any legislative "grant of authority to the executive in the domain of foreign affairs ought generally to include a power of interpretation." [FN197] Presumably, the authors mean that the Court should construe any treaty or foreign relations statute as implicitly delegating interpretive power. Yet such a delegation theory faces several hurdles. For example, it is not at all clear what "interpretive" power Congress has to delegate, as the Court has regularly drawn lines between the constitutional function of lawmaking and law interpreting. [FN198] Congress surely possesses the former, but not so obviously the latter. Indeed, it is for this reason that the more persuasive formal explanation for Chevron has been one that understands Congress as having delegated lawmaking power to the agencies (whether that delegation is express or implied). [FN199] As long as this is the case, executive agencies engaged in the business of statutory construction in the course of implementing Congress's instructions need not intrude on the judicial power at all; they *824 are acting only as a more detail-oriented extension of Congress itself. The notion that executive agencies post-Chevron are carrying out a core judicial function of law interpretation would present a far greater challenge to the formal judicial power than Sunstein and Posner's thesis appears to contemplate. In an era when the delegation doctrine, long thought dead, continues to find judicial support in various forms, [FN200] the authors' proposed solution risks the criticism that their functional cure will kill the formal patient.

Importing Chevron into the foreign relations setting without attempting to address the question of judicial power only perpetuates the formal interpretive debate. Particularly because the formal allocation of foreign relations power between the judicial and executive branches--unlike the more novel authority of administrative agencies--is a subject of express constitutional concern, it seems essential to have a formal theory of how interpretive power may be shared in this realm before designing a deference doctrine that effectively shares it. Once a "case or controversy" is properly before an Article III court, is there a formal floor of judicial power to interpret statutes and treaties, beneath which no functional deference rationale can allow the Court to sink? The remainder of the Article explores answers to this question of formal power in an attempt to shed light on which non-Chevron approach is appropriate.

II. Considering Formal Theories of the Judicial Power

The text of Article III of the Constitution is notoriously short on elaboration of what, precisely, is contained in the "judicial power of *825 the United States." [FN201] Chief Justice John Marshall's attempt in Marbury v. Madison [FN202] to put flesh on the bare bones of this power made some of its features clear, but arguably obscured others. While Marbury famously established that it was "the province and duty of the judicial department to say what the law is," [FN203] it also suggested that there were some executive actions that might not be amenable to judicial invalidation.
Moreover, while Marbury is understood to focus on why it is appropriate for the Court not only to engage in, but also to assert supremacy over, constitutional interpretation, the opinion devotes not a moment to justifying the Court's power to interpret the acts of Congress also at issue in the case.

In some respects, this relative inattention makes sense. Judicial interpretation of subconstitutional law arguably raises fewer concerns about the legitimacy of the judiciary, as it lacks the finality, and therefore the supremacy, associated with constitutional interpretation. If the regular democratic process has some capacity to fix any judicial mistake in the interpretation of a statute or treaty, then one need not worry as much about finding a democratic justification for judicial power. Yet it is still necessary to define the contours of the judicial power to interpret statutes and treaties to understand when the Court can decline to exercise its power or otherwise share power with another branch to interpret the law in cases properly before it. Largely in response to this need, presented most acutely by the rise of modern administrative law, scholars have explored a series of theories based variously on constitutional text and original meaning, as well as public choice and democratic theory, to explain why and to what extent judges have the power to say what subconstitutional law means. This Part reviews the two leading accounts of judicial interpretive power: faithful agent theory and what is often called instrumental theory. It concludes that while each account is instructive—and instrumental theory especially useful—neither ultimately seems sufficient for understanding the judicial role in interpreting foreign relations law.

A. Faithful Agent Theory

Likely still the dominant understanding of the courts' role in statutory interpretation, “faithful agent” theory sees the relationship between Congress and the courts as that of principal and agent, where the agent's duty is limited to discerning and applying the directions of the principal set forth in statute. As a theory of the judicial power, faithful agent theory has obvious attractions. The notion that judges act only as translators for the democratically elected legislature helps to address perennial concerns about the countermajoritarianism of an unelected federal judiciary. Indeed, the historical argument in favor of this view, set forth in detail by John Manning, contends that faithful agent theory is most consistent with the Constitution's structural efforts (driven in part by response to Anti-Federalist concerns) to address the countermajoritarian problem by limiting judicial discretion. Among other structural features, the Constitution's insistence upon bicameralism and presentment made it “difficult to imagine that the Founders designed an elaborate method of legislation, while simultaneously granting judges broad independent authority to alter the results outside that carefully constructed process.”

In Manning's account, the founding-era Marshall Court recognized the limited nature of the judicial role in this regard: “[I]t has truly been stated to be the duty of the court to effect the intention of the legislature.” This view led the Court away from the common law practice of equitable interpretation—construing otherwise-clear statutory texts to avoid injustice or to remedy textual gaps that seemed inconsistent with legislative policy. Moreover, Manning argues, to the extent the Court ever departed from the import of a plain text—by applying a substantive canon of interpretation, for example—such departures could be understood as necessary to fulfill the legislative intent. The canons of constitutional avoidance or of guarding against excessive delegations of power, for example, may “acquire a sort of prescriptive validity, since the legislature presumably has them in mind when it choosess its language.”

Yet faithful agent theory in other respects struggles to explain the use or value of such substantive canons—driven by extralegislative values—or the related use of clear statement canons, in which the Court requires a clear statement from Congress before interpreting a statute, for example, to infringe on state sovereignty or delegate excessive authority to another branch. Presumably, the theory could not tolerate the use of such canons to trump a reading of a statute whose tex-
tual meaning is otherwise plain. It likewise requires some explanation to understand how faithful agent theory could survive an executive deference doctrine like Chevron, which seemingly allows an executive agency to supplant the Court as the interpretive agent of Congress. Indeed, for the faithful agent understanding to work, Chevron must be understood not as a doctrine of judicial deference to executive authority, but rather as a doctrine of congressional authority alone. That is, when *828 the Court defers to an interpretation by an executive agency, it is deferring only because Congress has delegated the agency the authority of an adjunct legislature. [FN213] In this sense, the Court shows no deference at all to the executive, but rather just to the legislature-by-proxy.

Beyond the vigorous criticism to which faithful agent theory has been subject on historical and other grounds, [FN214] the theory for this reason seems particularly ill-suited to illuminate the judicial task of statutory interpretation in foreign relations law. Indeed, it is not clear that the theory leaves room for an executive interpretive role of any sort. Consider the faithful agent understanding of Chevron deference—an understanding that depends on an assessment of the executive’s superior political accountability as Congress’s delegated lawmaker. Yet political accountability (whether the agency is understood to be either a legislative delegate or part of an appropriately political executive administration) has only been part of the rationale for doctrines like Chevron. The other part—one central to the foreign relations context—is the notion that the executive possesses expertise that the Court may be wise to take into account, whether or not the legislature believes that it should. In this regard, it seems especially difficult to reconcile a view of the Court as a faithful agent to Congress with the expectation in foreign relations law that the executive’s views have at least some functional relevance to the task of law interpretation, whether or not Congress thinks they should. [FN215]

Using faithful agent theory to explain the judicial power in treaty interpretation is even more suspect. In the Manning vision, limiting the Court’s role to that of faithful agent is necessary to preserve the integrity of the Framers’ scheme that laws would be made only with bicameral approval and after presentment to the executive. Treaties, of course, *829 emerge from a formally different place, with the treaty-making power residing in the executive, but only “by and with the Advice and Consent of the Senate.” [FN216] At a minimum, the constitutional text would seem to give the executive some claim to a shared, but nonetheless formal, role in “making” the treaty law. Indeed, excluding all evidence of executive views in treaty making seems likely to diminish the accuracy of any judicial interpretation. Moreover, even if the Senate and executive were the sole lawmakers involved in treaty making, the absence of House participation in treaty ratification weakens the argument that faithful agent theory helps preserve bicameral or democratic decisionmaking in any pure sense. In any case, the executive and Senate are not the sole lawmakers involved in making treaties; foreign treaty partners help conceive, negotiate, and draft the legal text. In this context, it is a mistake to view the U.S. government or any of its branches as the sole “principal” lawmaker whose intent the Court must discern. [FN217]

Perhaps more significantly, a faithful agent view of treaty interpretation is inconsistent with an important theme in the Court’s historical approach to treaty interpretation, one that understands the judicial task as in part akin to contract interpretation, in which the intent that must be discerned is that of the treaty parties. [FN218] In this regard, the claim that the Court regularly defers to executive views on the meaning of treaties obscures more than it clarifies. [FN219] It is true that the Court has on occasion invoked rhetoric that the views of “the departments of government particularly charged with [treaty] negotiation and enforcement” are due “great weight.” [FN220] Yet, as the Court noted in the case first invoking the “great weight” standard and since, the weight may be accorded not only to the views of the executive but to those of all the parties that negotiated the treaty. [FN221] To the extent that the Court has attended to the executive’s views, it is more regularly to the views of both negotiating partners as evidence of negotiating intent and of post-ratification performance. In this context, understanding the Court to be an “agent” of the parties seems jarring at best.

*830 B. Instrumental Interpretation
A second model of the judicial power, sometimes called instrumental theory, holds that Article III courts were not created to be mere agents of Congress. Rather, the courts were meant to employ quintessentially judicial canons of interpretation and methods of legal reasoning that would help both to clarify ambiguous texts and to influence legislative drafting over time. [FN222] One of the most thorough recent accounts of this view comes from Jonathan Molot. He contends that the Framers understood judicial reasoning to be at least moderately constrained on its own terms by judicial principles such as stare decisis and by interpretive canons that drove courts to avoid absurd or unjust results. [FN223] In this view, courts bring to bear institutional and professional norms to help serve rule-of-law interests in consistency, fairness, justice, and rationality across the law--in order to "induce legislators to internalize these judicial values when enacting statutes in the first place." [FN224] Such interests were less likely to be reflected in legislation if the law's content was left only to the pull of political constituencies, driven by their own specific and immediate needs. [FN225] Moreover, independent judicial interpretation of statutes could prompt further public engagement with gaps in statutory meaning, whether the gap results from legislative inadvertence or a failure of political compromise. [FN226] In this *831 sense, courts' transparent exercise of the interpretive function could also serve a democracy-forcing function, helping to clarify the law (and thereby to promote the rule of law) over time.

Much in an instrumentalist theory of judicial power seems salient in foreign relations law. On formal grounds, there is the promise that judicial involvement could help reinforce a structural constitutional scheme that contemplates Congress and the executive sharing power in foreign relations. [FN227] Although the Constitution grants Congress any number of broad textual powers that seem to contemplate its engagement in and regulation of U.S. foreign affairs, [FN228] scholars have long lamented Congress's cession of power to the executive on many questions of foreign relations. This phenomenon may derive from political dynamics that tend to give the executive disproportionate political credit for engagement in foreign relations successes, while ensuring that both political branches are blamed for foreign relations failures. [FN229] But whether Congress's reticence is driven by constitutional conviction or political fear (or some other institutional failing), it *832 may be prompted into action by judicial insistence that Congress reengage in matters of foreign relations.

Indeed, Congress has demonstrated its capacity to respond when it dislikes the interpretive efforts of the Court. [FN230] The question about the legality of executive-made military commissions as a forum for war crimes trials in Hamdan is only a more recent example. The issue in Hamdan revolved around the President's authorization of the use of military commissions in late 2001. [FN231] For five years thereafter, Congress remained silent while the executive branch made repeated efforts to refine the commission structure in the face of vigorous objections. The Court's 2006 decision in Hamdan--holding, inter alia, that the President lacked the authority to convene such commissions without express congressional authorization [FN232]--compelled the executive to seek engagement by Congress. Congress thus entered a heated public debate on the question and ultimately passed a detailed statute authorizing the use of military commissions. [FN233] While the resulting Military Commissions Act of 2006 may be criticized on various levels, there is little question that it was the Court's engagement that forced serious legislative consideration of the parameters of commission trials. In this regard, judicial involvement promoted the structural value of political accountability: the Court's action forced a transparent debate in Congress, rather than leaving the resolution of core questions of meaning to far less transparent executive branch processes, where secrecy may readily disable accountability checks.

There is also much to be said about the utility of judicial pressure on the political branches to clarify foreign relations law and legal texts over time. Consider recent judicial efforts to interpret the AUMF, which Congress enacted in the wake of the attacks of September 11, 2001. [FN234] Given the relatively sparse legislative history and other standard *833 interpretive sources that usually help courts discern the meaning of statutes, some scholars have suggested that historical executive branch practice should be explored to shed light on statutory meaning. [FN235] If the President has interpreted force-authorization language one way in the past--and especially if Congress has acquiesced in that interpreta-
tion over time—then a later Congress could employ the same language comfortable in the knowledge that executive implementation would accurately reflect its intent. [FN236]

Yet, as the Court itself has recognized, reliance on acquiescence to past practice is fraught with problems that range from functional concerns about interpreting legislative silence to formal problems of according the same authority to congressional silences as to congressional legislation that has satisfied the important hurdles of bicameral debate and presentment to the executive. [FN237] In the foreign relations context, it may be especially unclear: whether a particular executive action is taken pursuant to an executive understanding of statutory delegation, or based on the executive's view of its own constitutional authority. And particularly if one believes modern security threats are categorically different from past dangers, it is not at all evident that past executive practice offers clarification in this realm. In contrast, a legislature acting in the shadow of clearer judicial expectations—or any guidance—in drafting statutes might facilitate legislative use-of-force debates, crystallizing differences in circumstances when prompt resolution may be important.

While adopting an instrumental theory of judicial power in foreign relations law may thus have considerable advantages, a purely instrumental view of structural judicial power leaves open some important questions for deference doctrine in foreign relations. A first set of questions goes to the permissibility of deference of any kind to executive views in statutory interpretation. The instrumentalist court's duty to ensure that legislative drafting is informed by rule-of-law values would seem to preclude much attention to executive views at any stage. Limiting judicial engagement in the interpretation of legal questions properly before the courts would curtail the infusion into *834 lawmaking of judicial values that instrumentalisists would maintain. The Framers expected the courts to promote. Instrumental theory might well tolerate judicial consideration of executive views (short of legal deference) for functional reasons—a Skidmore-like attention to the formal process, relative expertise, and persuasiveness of the executive's position. But it is difficult to see instrumental theory as readily reconcilable with even Chevron—much less Curtiss-Wright—deference to executive views. If instrumental theory as such is right, superdeference regimes are likely wrong.

Perhaps more importantly, instrumental theory leaves central questions about the relationship between the interpretive power of the courts and the executive unanswered. In particular, it does little to resolve the role of substantive canons of statutory construction, which faithful agent theory at least explains as fair inferences of legislative intent. [FN238] Would instrumental theory tolerate, require, or forbid an avoidance canon that requires a clear legislative statement before rendering an interpretation that has the effect of delegating power from one branch to another? [FN239] The instrumentalist court fulfills its duty, it seems, by promoting clarity in the law to serve general interests in fairness and the rule of law. In this regard, any weight executive views may carry could sway judicial decisionmaking, even if the executive's interpretation ran afoul of one of these substantive canons. Particularly in foreign relations law, where it has been argued that nondelegation canons, for example, may have less salience in the face of the executive's formal constitutional authority, [FN240] it seems important to understand whether part of the judicial power requires the Court to police substantive commitments, as well as interpretive ones.

*835 Instrumental theory, likewise, seems a partial description at best of the Court's role in treaty interpretation. It is hard to believe that the judicial power in treaty interpretation hinges on the expectation that interpretive values pursued by the U.S. judiciary alone are meant to have a clear impact on treaty drafting over time. After all, Congress does not hold the treaty-drafting pen, or it holds it only in an indirect way. While the executive certainly has some incentive to take Supreme Court interpretive expectations into account in negotiating treaty texts, in multilateral treaty negotiations, the United States is but one judicial system among many. Foreign courts are hardly bound by the interpretive guidance of the U.S. Supreme Court, and treaty partners have their own domestic interpretive demands to fulfill. [FN241] Under the circumstances, it would be surprising if instrumental influences of this sort were the primary expected judicial function in treaty interpretation.
The Supreme Court has a long history of vigorous engagement in treaty interpretation, beginning aggressively in the era of the founding of the United States. [FN242] But if not as faithful agent, and if not with purely instrumental goals in mind, what is the Court's understanding of its role in interpreting treaties? Put differently, what is the nature of the judicial power such that it extends to foreign relations law at all?

III. Exploring a Formal Theory of Judicial Power for Foreign Relations Law

Given the seeming inadequacies of primary theories of the judicial interpretive power to address the standard challenges of foreign relations law, the final part of this Article begins to explore theoretical frameworks that might avoid the failures of faithful agent theory in *836 this realm and fill in the gaps left by purely instrumental approaches. Here called equilibrium theory, this emerging model draws both on traditional justifications for judicial supremacy in constitutional interpretation and on scholars' attempts to reconcile formal notions of the separation of powers with the advent of the administrative state. In brief, the claim is that part of the judicial power is to promote the separation of powers. This Part first introduces the basic idea. It then considers the principal objection to the approach: in particular, the formal claim that the executive has its own interpretive power that must be taken into account in any understanding of shared interpretive authority. Throughout, this Part considers what such a view of the judicial duty would contribute to our understanding of deference in current dilemmas in statutory and treaty interpretation.

A. Equilibrium Theory

It is hardly new to suggest that the Supreme Court has a role to play in preventing the accrual of excessive power in any one branch of the federal government. Such a duty has been understood to emerge from a range of constitutional sources, from general principles of the separation of powers to specific guarantees of individual rights in the text. [FN243] Indeed, the argument that it is a core judicial function to police structural boundaries to constrain power is a central justification of Marbury itself:

This original and supreme will organizes the government, and assigns, to different departments, their respective powers. It may either stop here; or establish certain limits not to be transcended by those departments.

The government of the United States is of the latter description. The powers of the legislature are defined, and limited; and that those limits may not be mistaken, or forgotten, the constitution is written. To what purpose are powers limited, and to what purpose is that limitation committed*837 to writing, if these limits may, at any time, be passed by those intended to be restrained? The distinction, between a government with limited and unlimited powers, is abolished, if those limits do not confine the persons on whom they are imposed, and if acts prohibited and acts allowed, are of equal obligation. [FN244]

Of significance here, Marbury's message in this regard is not limited to constitutional interpretation but extends to statutory and treaty interpretation as well. [FN245] This understanding should be unremarkable. The text of Article III makes it clear that the "judicial power" extends without distinction to the Constitution, statutes, and treaties. [FN246] It is not immediately apparent why that power, to the extent it includes any interpretive authority, would not be exercised in largely the same way from one instrument to the next.

To the extent modern scholars have challenged Marbury's conception of judicial power in this regard—and challenged it they have—their concerns have focused principally on the particular dilemma of constitutional interpretation. The contemporary constitutional theory commonly labeled "departmentalism," for instance, holds that "each branch, or department, of government has an equal authority to interpret the Constitution in the context of conducting its duties" and "is supreme within its own interpretive sphere." [FN247] Drawing on textual, structural, and historical claims to shared in-
terpretive authority, departmentalists have advanced a range of reasons the political branches should be understood to have at least some power to interpret for themselves the meaning of the Constitution, including its structural grants of authority. [FN248] For these scholars, the principal objection to *838 Marbury's assumption of judicial supremacy is the countermajoritarian one: of all branches, why should the non-democratic Court have the power to say what our democratic Constitution means, particularly as it is so difficult to amend the Constitution democratically (as the Constitution itself provides)? Why should the Court be allowed effectively to end the debate on constitutional meaning?

For reasons that should be apparent, judicial interpretation of statutes and treaties poses less troubling democratic concerns. If Congress does not like the Court's interpretation of a statute, whether based on a substantive canon of interpretation or on some other reason, it can pass another one. If Congress does not like the Court's interpretation of a treaty, it can pass a subsequent statute, effectively overturning whatever interpretation the Court has given the treaty. [FN249] Indeed, as instrumental theories of judicial power suggest, judicial interpretation of statutes and treaties can serve an eminently democratic function, not only by compelling the lawmaker to clarify meaning through a public and deliberative process, but also by infusing laws with judicial values of stability and consistency. [FN250] Such a function is likely to be particularly valuable in certain foreign relations contexts, where executive branch secrecy can challenge the effectiveness of congressional oversight.

For statutes and treaties, then, the more significant challenge to the Marbury view of interpretive authority—a view that assumes some judicial role in limiting government power—is less a question of which single branch should play the role of interbranch enforcer. Instead, it is the challenge of identifying what those formal authorities are, or could be, in the modern administrative state. If executive agencies are to carry out both quasi-legislative and quasi-adjudicative functions, then an interpretation of Marbury (or anything else) that would contemplate the enforcement by any branch of a strictly formal division of *839 powers—executive power to the executive, legislative power to Congress, and so forth—cannot survive.

Yet the notion that federal power may be effectively limited only by, for example, preventing the executive from issuing any kind of legal rule (lest it be accused of legislating) was not necessarily the separation-of-powers concept the Framers had in mind or the limit Marbury itself necessarily contemplated. Rather, as Cynthia Farina noted in the wake of Chevron, the Madisonian vision of separated powers was of a government of shared authority, with each branch possessing enough constitutional power “to resist encroachments of the others.” [FN251] Allowing one branch to accrue functional authority over time in the service of effective governance was thus permissible as long as the other branches could respond with equal and opposite constraining forces of their own. Delegation of legislative power to the executive could be tolerated under this scheme, as long as it remained possible to maintain an offsetting power through independent judicial interpretation. [FN252] In this respect, the problem with Chevron was that it disabled that system of “dynamic equilibrium,” depriving the courts of their full power of interpretation just when the need to preserve equilibrium was greatest. [FN253]

If this view of the modern consequences of Marbury is correct—that is, the view that part of the judicial role is to help maintain interbranch equilibrium—it holds several implications for statutory and treaty interpretation that make it a useful supplement to an instrumental approach. First, like instrumental theory, the equilibrium view does not bar judicial consideration of an executive branch interpretation of a law, particularly insofar as the executive may enjoy expertise that might clarify legislative meaning. But unlike instrumental theory, the equilibrium model carries clear implications for the relative weight due to substantive canons of interpretation—like the nondelegation canon—as compared with claims of executive deference. Contemporary writings on whether the executive's view or a judicial canons should trump in cases of statutory ambiguity commonly see the canons as flowing from some combination of functional interests in judicial prudence, institutional minimalism, and administrative utility.*840 [FN254] And if nondelegation canons are driven
principally by functional concerns, then competing functional demands might trump the canons themselves— for example, the demand of deferring to executive expertise in foreign relations matters. [FN255] If, however, nondelegation canons are a necessary adjunct to the formal judicial power to interpret the law, then one might expect the Court to require at least a clear statement before it interprets a statute or treaty to effect the transfer or accretion of significant discretionary power. [FN256] An equilibrium theory approach would embrace the latter view. That is, when faced with ambiguity, the Court would give priority to interpretive canons that reduce the likelihood that any one branch would be barred from, or could shirk, continued participation in interbranch debate. To extend the example from above, a court considering the scope of detention authority provided by the 2001 AUMF would adhere to the substantive canon against delegation before simply deferring to executive views on grounds of expertise. [FN257]

Second, when a purely instrumental understanding of the judicial power seems an inadequate and therefore unlikely explanation for the Court's active role in treaty interpretation, equilibrium theory *841 would provide more meaningful guidance—leading the Court to disfavor constructions that disrupt interbranch equilibrium or otherwise enable the accretion of federal power through international law. In this respect the Medellín Court, for example, might be understood to have acted appropriately to reinforce equilibrium by rejecting the executive's argument that the IJC's judgment, although not binding in courts of its own authority, “became the law of the land with precisely the effect pursuant to the President's Memorandum and his power ‘to establish binding rules of decision that preempt contrary state law.’” [FN258] Recall that the executive's argument in Medellín was that the relevant treaties should be read to “implicitly” give the President the power to implement the United States' “treaty-based obligation” to effect compliance with the IJC's decision. [FN259] Rejecting the executive's proposed reading, the Court demanded a clearer statement—in the treaty or, perhaps more sensibly, from Congress itself—that this was indeed the desired effect. Absent such a statement, the Court would not permit the executive to claim a power, by treaty, to “convert[] a non-self-executing treaty into a self-executing one.” [FN260]

Equilibrium theory could also counter trends in international law and legal structures that may tend to increase the relative power of domestic executives within domestic legal structures. [FN261] Here, the Court's per curiam decision in Munaf v. Geren [FN262] should stand as a cautionary tale. In Munaf, the Court was reluctant to “second-guess” the executive's determination, based on close coordination between the U.S. State Department and the Iraqi Ministry of Justice, of the likelihood that two U.S. citizens would face torture if transferred to Iraqi custody. [FN263] The executive argued that such second-guessing “would require federal courts to pass judgment on foreign justice systems and undermine the Government's ability to speak with one voice in this *842 area.” [FN264] While the Court ultimately declined to reach directly the statutory and treaty interpretation questions that underpinned the habeas petitioners' request for relief, [FN265] a view that it is part of the judicial duty to promote interbranch equilibrium would likely require the Court to take a more active interpretive role.

B. Considering Formal Objections

As noted above, a view of the judicial power that affords the Court a formal role in promoting interbranch equilibrium would tend to trump the functional considerations of expertise on which most theories of executive deference are based. [FN266] For this reason, the most powerful arguments against an equilibrium theory of judicial power in foreign relations law are based not on the executive's functional expertise, but rather on formal claims about its Article II power. Article II offers the executive several fonts of authority, including the Commander-in-Chief Clause and the Treaty Clause, that may afford the President interpretive power in foreign relations matters that is not otherwise implicated in standard administrative law. [FN267] Yet while there is a good case to be made that the executive must have some inherent power to interpret statutes and treaties, it is far from clear that this power entitles the President to any more deference
than federal agencies enjoy under Skidmore. [FN268] Because an equilibrium theory understanding of judicial power poses no bar to the consideration of executive branch interpretations to this extent, recognizing some formal interpretive power in the executive may be broadly compatible with the judicial role described here.

Scholars have regularly argued that judicial deference to executive interpretations of foreign relations-related statutes and treaties is necessitated in part by the President's own formal constitutional authority.*843 In the statutory context, for example, Professors Bradley and Goldsmith have maintained that the executive should have fairly broad power to construe its “necessary and appropriate” authority under the 2001 AUMF, a statute that, as noted above, is now the subject of much judicial debate. [FN269] In addition to suggesting various reasons that the executive might be entitled to judicial deference, Bradley and Goldsmith contend that the executive's formal constitutional authority over foreign relations renders interpretive canons disfavoring broad delegations of power less salient. [FN270] Citing cases such as Loving v. United States, in which the Court upheld the President's authority under the UCMJ to prescribe aggravating factors for death penalty sentencing in courts-martial, the authors posit that “[t]he delegated duty . . . is interlinked with duties already assigned to the President by express terms of the Constitution, and the same limitations on delegation do not apply where the entity exercising the delegated authority itself possesses independent authority over the subject matter.” [FN271] Further, and more to the point, the authors contend, because the nondelegation doctrine is itself less of a concern, so too should be the nondelegation interpretive canon requiring a clear statement before assuming Congress intended to authorize a broad delegation of power. [FN272] Thus, while a statute delegating general power to the President to take certain action whenever it is “necessary and appropriate” might ordinarily pose delegation concerns, in this view such delegation concerns in the foreign relations context neither render the statute invalid nor even require that Congress clarify its intention before a court may interpret the statute's scope as broadly as the executive demands. [FN273]

One need not reject entirely the belief that the President has some formal authority to interpret and apply statutes to identify several reasons to doubt the ultimate persuasiveness of this claim. For one, the Court's reluctance to embrace nondelegation-doctrine challenges to executive actions pursuant to statutory authority may be less significant to the scope of formal executive authority in foreign relations than Bradley and Goldsmith assume. The modern Court's lack of receptivity to substantive nondelegation challenges is hardly limited to *844 the foreign relations context. As the Loving Court noted, “Though in 1935 we struck down two delegations for lack of an intelligible principle, we have since upheld, without exception, delegations under standards phrased in sweeping terms.” [FN274] While cases such as Loving and Curtiss-Wright may have once seemed notable and foreign relations-specific exceptions to an otherwise broadly applicable rule against recognizing broad delegations of legislative power, it should by now seem clearer that these cases are only a few examples of a far broader rejection of nondelegation challenges, entirely independent of questions of formal executive power in foreign relations.

Beyond this, in many of the cases Bradley and Goldsmith cite in support of their claim that the courts recognize that the executive's formal powers in foreign relations may flip standard canons of statutory interpretation, the Court has focused on the executive's relative functional superiority, not its formal authority. The 1965 passport-regulation dispute, Zemel v. Rusk, [FN275] is a case in point. There, the Court was called to consider a nondelegation challenge to a statute authorizing the Secretary of State to issue passports under rules prescribed by the President; the Secretary had interpreted the statute to authorize the restriction of travel to Cuba. [FN276] Paying modest attention (by Chevron standards) to the executive's views—noting only that “[t]he interpretation expressly placed on a statute by those charged with its administration must be given weight” [FN277]—the Court rejected the nondelegation challenge. Notably, its rejection was not couched in language evincing any concern for (or recognition of) some inherent formal authority of the executive but rather on the grounds that

because of the changeable and explosive nature of contemporary international relations, and the fact that the
Executive is immediately privy to information which cannot be swiftly presented to, evaluated by, and acted upon by the legislature, Congress—in giving the Executive authority over matters of foreign affairs—must of necessity paint with a brush broader than that it customarily wields in domestic areas. [FN278]

*845 While there can be no question that the Court has taken such functional considerations into account in construing statutory delegations of power to the executive and in resolving separation-of-powers questions more broadly, a recognition that such considerations may matter is a far cry from the position that the Court is compelled to take them into account by the executive’s authority under Article II. [FN279]

Perhaps more importantly, it is a significant—and unwarranted—conceptual leap to move from the (arguable) proposition that delegation doctrine is broadly less salient when construing foreign relations statutes [FN280] to the proposition that the interpretive canon against broad delegations should not apply, or the even broader proposition that *846 the Court’s role in interpretation may be appropriately ceded to the executive in this realm. Indeed, even as the substantive nondelegation doctrine has shriveled in importance in the modern administrative state, the Court has paid sustained attention to the nondelegation interpretive canon. [FN281] That the Court should prefer the interpretive canon as an approach to serving nondelegation interests in fact makes good sense. The substantive doctrine and interpretive canon serve different purposes and have different effects. A holding that Congress violates the separation of powers in overbroad delegations of authority to the President conclusively limits the government’s options. The interpretive canon allows Congress and the President the opportunity to pursue an arrangement of broadly delegated powers, but only if the effect of the arrangement is made clear through democratic deliberation and clear legislative commitment. Although the Court has largely declined to attach strong constitutional prohibitions to delegated-power arrangements, that does not mean it has lost interest in pursuing separation-of-powers goals through less constitutionally “nuclear” means. Any reluctance the Court feels in applying the substantive doctrine in the foreign relations context may not—and need not—carry over to its application of the interpretive canon.

Given the limitations of such doctrinal arguments, the stronger claim that formal executive power may preclude adherence to equilibrium theory in the interpretation of statutes and treaties may come by extension from the departmentalists, who maintain that the executive has at least some interpretive authority over the meaning of the constitutional law. [FN282] Recall that departmentalism holds that “each branch, or department, of government has an equal authority to interpret the Constitution in the context of conducting its duties” and “is supreme within its own interpretive sphere.” [FN283] Based on textual, structural, and historical claims to shared interpretive authority, [FN284] as well as on various strands of political theory including notions of popular constitutionalism, [FN285] the general idea may be succinctly summarized:

*847 Just as, under Marbury v. Madison, the obligation to decide cases consistently with the Constitution gives the Court the power and obligation of judicial review, so, too, the Constitution’s grant of executive power, together with the duty faithfully to execute the laws, means that the executive and Congress acting in their own spheres must interpret and apply the Constitution. [FN286]

While it is certainly true that aspects of the departmentalist rationale are strongly tied to the unique task of constitutional interpretation [FN287] and therefore are not necessarily instructive on the question of statutory and treaty interpretation at issue here, not all of the text-based arguments for departmentalism are limited to the interpretation of the Constitution. [FN288] Indeed, departmentalist reliance on the separation-of-powers idea that the power of interpretation is too important to be held exclusively by one branch cannot obviously be limited to constitutional interpretation per se. [FN289] It thus should not be surprising that some departmentalist scholars have suggested that their view of the executive’s formal interpretive authority extends to statutes and treaties as well. [FN290] The “judicial power,” [FN291] a term understood to encompass*848 an interpretive function, extends equally to the Constitution, statutes and treaties. Why would the “executive power,” if understood to encompass any interpretive function, be construed differently?
A weak version of the claim that the executive has some independent authority to interpret statutes and treaties is not especially objectionable. The executive must have at least some power to interpret the law, if only enough to "take care" that the law is implemented in the (frequent) absence of a controlling judicial opinion. [FN292] Whether the courts fail to resolve all interpretive questions because of structural limitations [FN293] or because of more prudential concerns, [FN294] it is clear that not all statutes and treaties needing enforcement will be subject to judicial construction. Indeed, this view seems unavailable in formal terms, as one might readily imagine the constitutional requirement for the executive to ensure that the laws are faithfully executed includes the power to do what is practically necessary to execute the laws, including determining the law's meaning. At the same time, this kind of interpretive authority does not generally threaten the "judicial power," a power limited by the express recognition that the federal courts will decide only those disputes concrete enough to constitute a case or controversy. [FN295] Accepting that the executive has some interpretive power of this sort does not imply an answer to the question of whether this power in foreign relations matters should preclude the Supreme Court from exercising a duty to apply its own interpretive power to preserve interbranch equilibrium.

*849 A stronger version of the departmentalist idea, however, challenges not only judicial exclusivity in interpretation, but also judicial supremacy: the assumption that the Court necessarily wins the interpretive battle of the branches. In this view, where a particular power is textually committed to the executive alone, such as the power to issue pardons or veto legislation, the executive should enjoy supremacy in determining how to interpret these powers. [FN296] Some departmentalists contend that the President must thus have the authority to decline to enforce statutes he believes are unconstitutional. [FN297] An even broader view suggests that the President's interpretive authority entitles him to refuse to comply with orders of the courts. [FN298] While such claims remain a minority view, [FN299] it is not difficult to imagine the implications of such a view for statutory and treaty interpretation: if the executive can fully ignore laws he thinks are bad, then his interpretation of those laws should have some primacy even if only to avoid such a dramatic step. Indeed, it is precisely this argument that John Yoo, among others, has advanced with respect to treaty interpretation—specifically, that the Constitution grants the President exclusive control over treaty interpretation by vesting the executive power in the President and by granting the President power to make treaties. [FN300]

*850 Yoo's account is plagued by several flaws, [FN301] not the least of which is that it is difficult or impossible to establish which, if any, of the executive's foreign relations powers are exclusive. The executive's power to make treaties is coupled with the Senate's power to ratify them. [FN302] The Constitution equally defines the "judicial Power" as extending to "all Cases . . . arising under this Constitution, the Laws of the United States, and Treaties made." [FN303] And the courts certainly have a long history of behaving as though treaty interpretation is a power shared with the judicial branch. [FN304] With respect to the Commander-in-Chief power—arguably the most relevant formal duty "interlinked with" the statutory power contained in the AUMF—scholars have recently shown, in exhaustive detail, that Congress has historically been "an active participant in setting the terms of battle (and the conduct and organization of the armed forces . . .)," an assertion of shared power that the executive has most often accepted as within Congress's authority. [FN305] Departmentalism may give the executive strong claims to formal interpretive authority where it is clear his is the only source of constitutional power, but wherever power is shared, as in the realm of foreign relations, the task of maintaining equilibrium seems relevant.

*851 Conclusion

In many respects, the tendency of scholars and courts to view treaties and foreign relations statutes as a separate species of law is unfortunate. While it may have once been possible to draw a bright line between the tasks of governing that were purely domestic and those that arose uniquely in the realm of foreign relations, transformations in areas from
international trade and communications to biology and warfare to international law and legal structures render the easy distinction between foreign and domestic power increasingly quaint. The Supreme Court's active engagement with resolving foreign relations-related legal disputes in recent years may be seen as one manifestation of this broader trend. At the same time, considering foreign relations as a quasi-distinct body of law may continue to offer heuristic benefits. Among these benefits is the opportunity to evaluate dominant models of the judicial power against a particular set of examples that these models were not necessarily conceived to address. This Article has suggested that one lesson of this evaluation is to require the development of some additional understanding of the role of the courts in law interpretation.

Beyond such theoretical considerations, the question this Article addresses is one of intense practical concern over a novel question faced by contemporary courts: in construing a statute authorizing the President to use "necessary and appropriate force" to battle international terrorism, whose view of the meaning of "necessary and appropriate" controls? By arguing for an equilibrium-promoting concept of judicial power, the intent here has not been to discount the many reasons why the courts may wish to, and should, attend closely to the executive's views. The executive's functional strengths--its access to bodies of experts across the U.S. government and its experience in both applying the law on the ground day-to-day and applying its understanding of its own duties and political demands--make its views indisputably worth consideration. Rather, the point of this Article is to argue that it is possible for the courts to take such insights into account without precommitting their own interpretive exercise in categorical deference to any position the executive might take. Indeed, this Article has contended that such categorical deference is not formally required (as a matter of executive power) and may be formally prohibited (as a matter of judicial power).

Given the practical concerns driving this inquiry, it is fair, in the end, to wonder whether such a conclusion--effectively leaving the courts to determine the extent to which the executive's interpretation has "the power to persuade"--is bound to leave the courts more confused and less constrained than they already are. It is an intriguing question for empirical study. But the outcome is far from obvious. The courts are consistently in the business of conducting multi-factor analyses in the style of Skidmore to determine whether a search was reasonable, whether a defendant was afforded all process due, and a host of other inquiries. The Skidmore factors that contribute to persuasiveness are themselves a finite set. And in the end, the most meaningful constraints on the judicial power are most likely to come from the same powers that hold the executive and Congress in check: the dynamic and ongoing struggle among the branches.

[FN1]. Visiting Faculty Fellow, University of Pennsylvania Law School, 2009-2011; Associate Research Scholar, Woodrow Wilson School of Public and International Affairs, Princeton University. The author wishes to thank Paul Frymer, Kim Lane Scheppele, Anne-Marie Slaughter, and the Program in Law and Public Affairs at Princeton University for their support during the preparation of this Article. Thanks also to Mark Brandon, Robert Chesney, Christopher F. Chyba, Cary Coglianese, Martin Flaherty, David Fontana, Vicki Jackson, Ralf Michaels, Martha Minow, Catherine Stuve, and Jeffrey K. Tulis, as well as participants in faculty workshops at the Georgetown University Law Center, University of Pennsylvania Law School, and University of Georgia Law School for helpful discussions. Special thanks to Nandu Machiraju and Dan Firger for research assistance.

[FN2]. See Hamdi v. Rumsfeld, 542 U.S. 507, 516-19 (2004) (plurality opinion) (finding that the AUMF permits detention, at a minimum, of individuals who were "part of or supporting forces hostile to the United States or coalition partners" in Afghanistan and who are engaged in "an armed conflict against the United States") (quoting Brief for Respondent at 3, Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696))).
[FN3]. Hamily v. Obama, 616 F. Supp. 2d 63, 69 (D.D.C. 2009) (quoting Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803)); see also id. (“Although there is some disagreement regarding the extent of the deference owed the Executive in this setting, it is beyond question that some deference is required.”). The court also cites articles reflecting the scholarly debate on deference:

Compare Eric A. Posner & Cass R. Sunstein, Chevronizing Foreign Relations Law, 116 Yale L.J. 1170, 1220 (2007) (arguing that with respect to the AUMF, “the President should be taken to have the authority to interpret ambiguities as he chooses”), with Derek Jinks & Neal Katyal, Disregarding Foreign Relations Law, 116 Yale L.J. 1230, 1234 (2007) (acknowledging that under existing doctrines deference is warranted in some circumstances, but arguing that “increased judicial deference to the executive in the foreign relations domain is inappropriate”).

Id. at 69.

[FN4]. See, e.g., Department of Justice Oversight: Preserving Our Freedoms While Defending Against Terrorism: Hearings Before the S. Comm. on the Judiciary, 107th Cong. 162 (2002) (statement of Laurence H. Tribe, Tyler Professor of Constitutional Law, Harvard Law School) (“[C]ourts necessarily see but one case at a time and in wartime tend to defer to the executive’s greater knowledge and expertise...”); Louis Henkin, Foreign Affairs and the United States Constitution 132 (2d ed. 1996) (“Foreign affairs make a difference. Here, the courts are less willing than elsewhere to curb the federal political branches, are even more disposed to presume the constitutional validity of their actions and to accept their interpretations of statutes, and have even developed doctrines of special deference to them.”); Christina E. Wells, Questioning Deference, 69 Mo. L. Rev. 903, 906 & n.14 (2004) (citing various sources).

[FN5]. Sanchez-Llamas v. Oregon, 548 U.S. 331, 353-54 (2006) (quoting Marbury, 5 U.S. (1 Cranch) at 177); see also Medellín v. Texas, 552 U.S. 491, 523 (2008) (rejecting the executive’s argument that a judgment of the International Court of Justice, although not binding in courts of its own authority, “became the law of the land with precisely that effect pursuant to the President’s Memorandum and his power ‘to establish binding rules of decision that preempt contrary state law’” (quoting Brief for United States as Amicus Curiae Supporting Petitioner at 5, Medellin, 552 U.S. 491 (2008) (No. 06-0984))).


[FN10]. See infra Part I.

[FN12]. See Robert M. Chesney, Disaggregating Deference: The Judicial Power and Executive Treaty Interpretations, 92 Iowa L. Rev. 1723, 1772-73 (2007) (proposing a model of deference to executive treaty interpretation that varies based on the circumstances); Jinks & Katyal, supra note 3, at 1236-38 (recognizing that while some judicial deference is often appropriate, it is not appropriate when international law seeks to constrain the executive itself).


[FN14]. Posner & Sunstein, supra note 3, at 1217.

[FN15]. See infra subsection I.B.2.


[FN18]. See infra Section II.A.


[FN21]. See, e.g., William N. Eskridge, Jr., Dynamic Statutory Interpretation 116-18 (1994) (discussing the belief of the Framers of the Constitution in judicial engagement in interpretation); Jonathan T. Molot, The Judicial Perspective in the Administrative State: Reconciling Modern Dogmas of Deference with the Judiciary's Structural Role, 53 Stan. L. Rev. 1, 7 (2000) (arguing that judicial influence over legislative behavior is "an important component of the Founders' constitutional design").

[FN22]. A number of scholars have discussed the role of so-called normative canons in statutory interpretation. See, e.g., William N. Eskridge, Jr. & Philip P. Frickey, Quasi-Constitutional Law: Clear Statement Rules as Constitutional Lawmaking, 45 Vand. L. Rev. 593, 598 (1992) ("A good many of the substantive canons of statutory construction are directly inspired by the Constitution...."); Cass R. Sunstein, Law and Administration After Chevron, 90 Colum. L. Rev. 2071, 2111 (1990) ("By using these principles, courts decide cases of statutory meaning by reference to something external to legislative desires....").


[FN25]. Id. at 2.

[FN27]. Farina, supra note 17, at 496-97 (quoting The Federalist No. 51, at 349 (James Madison) (Jacob E. Cooke ed., 1961)).

[FN28]. See id. at 487 (explaining how judicial review can help check excessive delegations of power).

[FN29]. Id. at 497.


[FN32]. See, e.g., Bradley & Goldsmith, supra note 23, at 2100 (noting that the AUMF governs a context in which the President "possesses independent constitutional authority under Article II," so "the authorization need not be as precise as would be required in the absence of concurrent presidential authority").


[FN34]. See sources cited supra note 4 for examples of scholarly opinion describing deference to executive views.


[FN36]. See David J. Bederman, Deference or Deception: Treaty Rights as Political Questions, 70 U. Colo. L. Rev. 1439, 1462-66 (1999) (arguing that judicial deference in treaty interpretation increased during the twentieth century); Bradley, supra note 11, at 659 ("Since early in the nation's history, courts have been reluctant to contradict the executive branch in its conduct of foreign relations."); Scott M. Sullivan, Rethinking Treaty Interpretation, 86 Tex. L. Rev. 777, 780 (2008) (positing that twentieth-century courts regularly deferred to executive actions in foreign affairs).

[FN37]. See sources cited supra note 36.

[FN38]. Recent historical analysis of the founding-era Court finds no tradition of judicial deference to executive views on the meaning of treaties. See David Sloss, Judicial Deference to Executive Branch Treaty Interpretations: A Historical Perspective, 62 N.Y.U. Ann. Surv. Am. L. 497, 502-22 (2007) (surveying the Supreme Court's historically nondeferential approach to treaty interpretation). In statutory interpretation, scholars have long worked to demonstrate that the political question doctrine, for example, has given the Supreme Court little pause in practice. See Thomas M. Franck, Political Questions/Judicial Answers 61 (1992) (arguing that the political question doctrine has played a minimal role in Supreme Court case law and "may be falling into desuetude").

[FN39]. Kolovrat v. Oregon, 366 U.S. 187, 194 (1961); see also Sumitomo Shoji Am., Inc. v. Avagliano, 457 U.S. 176, 184-85 (1982) ("Although not conclusive, the meaning attributed to treaty provisions by the Government agencies charged with their negotiation and enforcement is entitled to great weight." (citing Kolovrat, 366 U.S. at 194)); Factor v. Laubenheimer, 290 U.S. 276, 285 (1933) ("[T]he resolution doubts the construction of a treaty by the political department of the government, while not conclusive upon courts called upon to construe it, is nevertheless of weight."); Sullivan v. Kidd, 254 U.S. 433, 442 (1921) ("[T]he construction placed upon the treaty before us and consistently adhered to by the
Executive Department of the Government, charged with the supervision of our foreign relations, should be given much weight.”); Charlton v. Kelly, 229 U.S. 447, 468 (1913) (”A construction of a treaty by the political department of the Government...is... of much weight.”).

[FN40]. See, e.g., Sumitomo, 457 U.S. at 184-85 (cautioning that agency interpretations are “not conclusive”).


[FN43]. Bradley, supra note 11, at 701.

[FN44]. See Chesney, supra note 12, at 1752-58 (reviewing treaty deference cases and concluding that the executive branch's interpretation "prevails in most instances").


[FN46]. Id.

[FN47]. Id. at 319.

[FN48]. Id.

[FN49]. See Bradley & Goldsmith, supra note 23, at 2100-01 (“[T]he same limitations on delegation do not apply where the entity exercising the delegated authority itself possesses independent authority over the subject matter.”) (quoting Loving v. United States, 517 U.S. 748, 772 (1996)).

[FN50]. See, e.g., Charles A. Lofgren, United States v. Curtiss-Wright Export Corporation: An Historical Reassessment, 83 Yale L.J. 1, 28-32 (1973) (criticizing the decision and its resulting impact).

[FN51]. See William N. Eskridge, Jr. & Lauren E. Baer, The Continuum of Deference: Supreme Court Treatment of Agency Statutory Interpretations from Chevron to Hamdan, 96 Geo. L.J. 1083, 1098-1100 (2008) (describing a continuum of judicial deference regimes, along which Curtiss-Wright-type attention to executive views appears at the most deferential end); see also Bradley & Goldsmith, supra note 23, at 2101-02 (citing Curtiss-Wright in support of broad readings of congressional delegations of power to the executive in foreign affairs).

[FN52]. Eskridge and Baer's survey of 1014 Supreme Court cases since Chevron in which an agency interpretation of a statute was at issue classifies only nine of these as foreign affairs and national security matters receiving "super-strong deference"--cases in which "the executive department interpretation prevails not only" when the statute is ambiguous, "but also in cases where Congress has not clearly trumped the agency or presidential construction." Eskridge & Baer, supra note 51, at 1101-02 & n.56. But even in these nine cases, it is debatable whether the executive's position prevailed because the Court deferred to an executive interpretation of a statute rather than reaching that result based on its own independent analysis. For example, one of the nine cases, Jama v. Immigration & Customs Enforcement, 543 U.S. 335 (2005), announced no deference scheme and conducted a thorough de novo exercise in statutory interpretation, noting only at the end that a "policy of deference" to the executive in foreign affairs would also lead it to favor the interpretation already given. Id. at 348. Another of the nine, Cheney v. United States District Court, 542 U.S. 367 (2004), involved the
interpretation of the common law writ of mandamus and common law executive privilege.


[FN55]. Breard, 523 U.S. at 375-76 (holding that state procedural rules can trump a defendant’s collateral assertion of Vienna Convention rights).


[FN57]. LaGrand Case (Ger. v. U.S.), 2001 I.C.J. 466, 498 (June 27) (quoting Vienna Convention on Consular Relations, supra note 53, art. 36(2)); see also Avena and Other Mexican Nationals (Mex. v. U.S.), 2004 I.C.J. 12, 43 (Mar. 31) (finding a duty to give a detainee notice of Article 36 rights once there is a strong reason to believe the person is a foreign national).

[FN58]. 548 U.S. at 340.

[FN59]. See id. at 345-50.

[FN60]. Id. at 346 (quoting 1 Restatement (Third) of Foreign Relations Law of the United States § 325(1) (1987)).

[FN61]. Id. at 353. Because the Court ruled against habeas petitioners on the remedy question, it concluded it did not need to reach the third question presented in the case: “whether Article 36 of the Vienna Convention grants rights that may be invoked by individuals in a judicial proceeding.” Id. at 342-43.

[FN62]. Id. at 353-55.

[FN63]. Id. at 353-54 (quoting Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803)) (citing Williams v. Taylor, 529 U.S. 362, 378-79 (2000) (opinion of Stevens, J.) (“At the core of [the judicial] power is the federal courts’ independent responsibility—indepenedent from its coequal branches in the Federal Government, and independent from the separate authority of the several States—to interpret federal law.”)).

[FN64]. Id. at 354-55 (quoting Kolovrat v. Oregon, 366 U.S. 187, 194 (1961)).

[FN65]. Id. at 355.


[FN67]. Sanchez-Llamas, 548 U.S. at 355 (quoting Memorandum from President George W. Bush, supra note 66).

[FN69]. See id. at 506-07 ("The interpretation of a treaty, like the interpretation of a statute, begins with its text. Because a treaty ratified by the United States is 'an agreement among sovereign powers,' we have also considered as 'aids to its interpretation' the negotiation and drafting history of the treaty as well as 'the postratification understanding' of signatory nations." (quoting Zicherman v. Korean Air Lines Co., 516 U.S. 217, 226 (1996) (citation omitted))).

[FN70]. Id. at 513 (quoting Sumitomo Shoji Am., Inc. v. Avagliano, 457 U.S. 176, 185 (1982)).

[FN71]. Id. at 523 (quoting Brief for United States as Amicus Curiae Supporting Petitione, supra note 5, at 5).

[FN72]. Id. at 525 (quoting Brief for United States as Amicus Curiae Supporting Petitione, supra note 5, at 11).

[FN73]. Id.

[FN74]. Id. at 526.

[FN75]. See supra note 39 (citing cases in which the Court considered executive negotiating history and performance).


[FN78]. See Kowlovat v. Oregon, 366 U.S. 187, 194-95 (1961) ("We have before us statements, in the form of diplomatic notes exchanged between the responsible agencies of the United States and of Yugoslavia, to the effect that the 1881 Treaty, now and always, has been construed as providing for inheritance by both countries' nationals without regard to the location of the property to be passed or the domiciles of the nationals.").

[FN79]. Sumitomo Shoji America, Inc. v. Avagliano, 457 U.S. 176 (1982), is especially direct in this regard. There, the Court reviewed evidence of both U.S. and Japanese intent to decide whether female employees' Title VII discrimination claim against an American subsidiary of a Japanese company was effectively precluded by the terms of the Friendship, Commerce and Navigation Treaty between the United States and Japan. See id. at 185-89.

[FN80]. Id. at 185 (emphasis added). Indeed, it was on this basis that Justice Scalia dissented in a later treaty interpretation case, arguing not that insufficient deference was paid to the United States' position but that "[w]hen we interpret a treaty, we accord the judgments of our sister signatories 'considerable weight.'" Olympic Airways v. Husain, 540 U.S. 644, 658 (2004) (Scalia, J., dissenting) (emphasis added) (quoting Air France v. Saks, 470 U.S. 392, 404 (1985)).


[FN83]. See id. at 584-85 (addressing the Government's argument that the Court should apply the "judge-made rule that civilian courts should await the final outcome of on-going military proceedings before entertaining an attack on those proceedings" (quoting Brief for Respondents at 12, Hamdan v. Rumsfeld, 548 U.S. 557 (2006) (No. 05-0184))); see also id. at 587-88 (finding that the commission review system "clearly lack[s] the structural insulation from military influence
that characterizes the Court of Appeals for the Armed Forces, and thus bear[s] insufficient conceptual similarity to state courts to warrant invocation of abstention principles").

[FN84]. Id. at 588 (quoting Ex parte Quirin, 317 U.S. 1, 19 (1942)); see also id. at 589 (concluding that despite the executive's claims of military necessity, "the Government has identified no other 'important countervailing interest' that would permit federal courts to depart from their general 'duty to exercise the jurisdiction that is conferred upon them by Congress'" (quoting Quackenbush v. Allstate Ins. Co., 517 U.S. 706, 716 (1996) (Kennedy, J., concurring))).

[FN85]. See id. at 625-35 (describing the executive's argument).

[FN86]. Id. at 630-32.

[FN87]. See id. at 635 ("Common Article 3 obviously tolerates a great degree of flexibility in trying individuals captured during armed conflict; its requirements are general ones, crafted to accommodate a wide variety of legal systems. But requirements they are nonetheless. The commission that the President has convened to try Hamdan does not meet those requirements.").


[FN89]. See 50 U.S.C. § 1541 note (2006) (authorizing the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided" the September 11, 2001, terrorist attacks).

[FN90]. Brief for Respondents at 24 n.9, Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696). To be clear, the executive's claim was not that the Court should defer to a particular determination by the President of a particular detainee's eligibility for POW status on the facts. Rather, this was a generalized conclusion about the relevance of the Convention to a conflict between two state parties to the treaty (the United States and Afghanistan). See id. at 12 ("[T]he nature of judicial review available with respect to the military's enemy-combatant determination is limited by the profound separation-of-powers concerns implicated by efforts to second-guess the factual basis for the exercise of the Commander in Chief's authority to detain a captured enemy combatant in wartime.").

[FN91]. The plurality made it clear that it was limiting its reading of the AUMF detention authority to the particular facts of Hamdi's case. See Hamdi, 542 U.S. at 516 (plurality opinion) (adopting, "for purposes of this case," the government's definition of an "enemy combatant" as one who was "part of or supporting forces hostile to the United States or coalition partners in Afghanistan and who engaged in an armed conflict against the United States there" (quoting Brief for Respondents, supra note 90, at 3)).

[FN92]. Id. at 521.

[FN93]. Id. at 518 (quoting Ex parte Quirin, 317 U.S. 1, 30 (1942)).

[FN94]. Id. at 519.

[FN95]. Id. at 521.

[FN96]. Id. at 535 (citing Korematsu v. United States, 323 U.S. 214, 233-34 (1944) (Murphy, J., dissenting) ("[L]ike other claims conflicting with the asserted constitutional rights of the individual, the military claim must subject itself to the judicial process of having its reasonableness determined and its conflicts with other interests reconciled."); Sterling v.
Constantin, 287 U.S. 378, 401 (1932) ("What are the allowable limits of military discretion, and whether or not they have been overstepped in a particular case, are judicial questions.").


[FN98]. See id. at 475 ("Respondents' primary submission is that the answer to the jurisdictional question is controlled by...Eisentrager."); see also Brief for Respondents at 14-25, Rasul, 542 U.S. 466 (2004) (Nos. 03-0334, 03-0343) (citing Johnson v. Eisentrager, 339 U.S. 763 (1950), as controlling precedent). Among other arguments, the government contended that the presumption against extraterritorial application of statutes ""has special force when we are construing treaty and statutory provisions that may involve foreign and military affairs for which the President has unique responsibility."" Id. at 19 (quoting Sale v. Haitian Ctrs. Council, Inc., 509 U.S. 155, 188 (1993) (Blackmun, J., dissenting)).

[FN99]. See Rasul, 542 U.S. at 487 ("From a practical perspective, the indefinite lease of Guantanamo Bay has produced a place that belongs to the United States, extending the 'implied protection' of the United States to it." (quoting Eisentrager, 339 U.S. at 777-78)). Because "sovereignty" per se was not the touchstone of jurisdictional authority, the executive's interpretation of the U.S.-Cuba lease agreement (allowing Cuba to retain "ultimate sovereignty") in this regard was similarly irrelevant.


[FN103]. Id. at 18 (quoting Uniform Code of Military Justice, 10 U.S.C. § 836 (2006)).

[FN104]. Id.

[FN105]. Id. at 47 n.22 (quoting Military Order of Nov. 13, 2001: Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 3 C.F.R. 918 (2009)).

[FN106]. See Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 865-66 (1984) (holding that when a statute's meaning is ambiguous, the Court will defer to the agency's judgment as long as it is reasonable); see also United States v. Mead Corp., 533 U.S. 218, 229 (2001) (clarifying the scope of Chevron deference to require a delegation by Congress of authority to make regulations "with the force of law.").

[FN107]. Hamdan, 548 U.S. at 622.


[FN109]. Hamdan, 548 U.S. at 622.

[FN110]. 10 U.S.C. § 836(b) (emphasis added).

[FN111]. Hamdan, 548 U.S. at 623.

[FN112]. Id.

[FN113]. Id. at 623 n.51.
[FN114]. Id. at 623.

[FN115]. Id. at 624.


[FN117]. See id. at 789 (concluding there was "no way to construe the statute to allow what is also constitutionally required in this context: an opportunity for the detainee to present relevant exculpatory evidence that was not made part of the record in the earlier proceedings"); see also id. at 792 ("To hold that the detainees at Guantanamo may, under the DTA, challenge the President's legal authority to detain them, contest the CSRT's findings of fact, supplement the record on review with exculpatory evidence, and request an order of release would come close to reinstating the § 2241 habeas corpus process Congress sought to deny them. The language of the statute, read in light of Congress's reasons for enacting it, cannot bear this interpretation.").

[FN118]. See id. at 796 ("In considering both the procedural and substantive standards used to impose detention to prevent acts of terrorism, proper deference must be accorded to the political branches."). Yet, from his mention of deference, Justice Kennedy drew at most a conclusion of policy, not one of interpretation: "The law must accord the Executive substantial authority to apprehend and detain those who pose a real danger to our security." Id. at 797. Beyond that, the opinion is notably obscure on how deference is to be accorded and to whom. One most easily reads Justice Kennedy as understanding the deference obligation to go to Congress and the President—not to the executive alone. Indeed, far from embracing traditional deference-like justifications, such as the danger that court involvement would risk embarrassment of multifarious pronouncements from different branches, Justice Kennedy insisted that the exercise of executive authority is "vindicated, not eroded, when confirmed by" courts. Id. Moreover, Justice Scalia categorically rejected the notion that the Court's posture was deferential in any regard. On the contrary, Scalia found Justice Kennedy's approach "a pose of faux deference to Congress and the President...What the Court apparently means is that the political branches can debate, after which the Third Branch will decide." Id. at 830 n.1 (Scalia, J., dissenting).


[FN120]. Id. at 703 n.6 (citing the Foreign Affairs Reform and Restructuring Act of 1998, Pub. L. No. 105-277, § 2242(a), 112 Stat. 2681-822, and the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment art. 3, registered June 26, 1987, S. Treaty Doc. No. 20 (1988), 1465 U.N.T.S. 85 ("No State Party shall expel, return (refouler) or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture.").

[FN121]. Id. at 700.


[FN123]. Id. at 23.

[FN124]. Munaf, 553 U.S. at 702.


[FN126]. See, e.g., Posner & Sunstein, supra note 3, at 1176 (arguing that courts should defer to the executive's foreign
policy expertise); Sunstein, Administrative Law Goes to War, supra note 11, at 2671 (arguing for a generous interpretation of presidential powers).

[FN127]. See, e.g., Bradley & Goldsmith, supra note 23, at 2084 (proposing to provide “a more systematic account” of the factors “relevant to interpreting the AUMF”); Chesney, supra note 12, at 1727 (lamenting that “the deference doctrine appears more unsettled and indeterminate than ever before”); Sullivan, supra note 36, at 781 (noting that courts have “failed to provide any clarity in [the] doctrine” for determining what degree of deference is appropriate).


[FN130]. Id. at 843.

[FN131]. Posner & Sunstein, supra note 3, at 1222.

[FN132]. Bradley, supra note 11, at 673. Note, however, that since Bradley's article was published in 2000, several new Justices have been confirmed to the Court.

[FN133]. See id. at 668, 773-75 (discussing disadvantages of a multifactor approach and advantages of Chevron). But see Thomas W. Merrill, Judicial Deference to Executive Precedent, 101 Yale L.J. 969, 970 (1992) (arguing that the Court continued to rely on multifactor tests despite Chevron).

[FN134]. Bradley, supra note 11, at 673 (footnotes omitted).

[FN135]. Posner & Sunstein, supra note 3, at 1206-07 (noting that the executive is far more politically accountable than the courts in the face of foreign policy crises).

[FN136]. Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803); see also, e.g., Stephen Breyer, Judicial Review of Questions of Law and Policy, 38 Admin. L. Rev. 363, 370 (1986) (describing the assumption that Congress delegates lawmaking power to the executive agency as a “legal fiction”); Sunstein, Beyond Marbury, supra note 11, at 2589 (describing Chevron as “a kind of counter-Marbury for the administrative state”).

[FN137]. Eskridge & Baer, supra note 51, at 1090. In the vast majority of the 1014 cases the Court decided during this period in which an executive agency interpretation of a statute was at issue, the Court applied either less stringent deference than that afforded by Chevron, or no apparent deference at all. Id. at 1121.


[FN139]. Chevron, 467 U.S. at 844 (quoting United States v. Shimer, 367 U.S. 374, 382 (1961)); see also id. at 865 (“Judges are not experts in the field....”).

[FN140]. Chevron, 467 U.S. at 843 n.9.

[FN142]. See, e.g., Eskridge & Baer, supra note 51, at 1086-87 ("Almost immediately, Reagan Administration officials and appointees proclaimed a 'Chevron Revolution.'"); Merrill, supra note 133, at 976 ("Justice Stevens'[s] opinion contained several features that can only be described as 'revolutionary,' even if no revolution was intended at the time." (quoting Kenneth W. Starr, Judicial Review in the Post-Chevron Era, 3 Yale J. on Reg. 283, 284 (1986))); see also Sunstein, Beyond Marbury, supra note 11, at 2596 (describing Chevron and McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316 (1819), as giving broad discretion to the executive to choose how to interpret statutes).

[FN143]. Chevron, 467 U.S. at 865.

[FN144]. Id. at 866.


[FN146]. Id. at 448 (rejecting the interpretation put forward by the Immigration Judge and BIA).

[FN147]. Id. at 447-48 (citations omitted in Cardoza-Fonseca) (quoting Chevron, 467 U.S. at 843 n.9) (internal quotation marks omitted).

[FN148]. Id. at 454 (Scalia, J., concurring).

[FN149]. Id.

[FN150]. See, e.g., Sunstein, Beyond Marbury, supra note 11, at 2604 ("Taken on its face, Cardoza-Fonseca seems to be an effort to restore the pre-Chevron status quo by asserting the primacy of the judiciary on purely legal questions.").

[FN151]. See, e.g., United States v. Meadow Corp., 533 U.S. 218, 226-27 (2001) (holding that Chevron deference only applies to statutory interpretation where Congress delegates the agency authority to make rules with "the force of law"); Christensen v. Harris Cnty., 529 U.S. 576, 587 (2000) (holding that interpretations in opinion letters do not warrant Chevron deference because, like interpretations in policy statements, manuals, or guidelines, they lack the force of law).

[FN152]. Mead, 533 U.S. at 221.

[FN153]. Id.

[FN154]. Mead, 533 U.S. at 233. The Court supported this conclusion with the observations that "Customs does not generally engage in notice-and-comment practice when issuing [ruling letters], and their treatment by the agency makes it clear that a letter's binding character as a ruling stops short of third parties." Id.


[FN156]. Id.


[FN158]. Christensen v. Harris Cnty., 529 U.S. 576, 587 (2000) (quoting Skidmore, 323 U.S. at 140); see also Skidmore,
323 U.S. at 140 ("[T]he rulings, interpretations and opinions of the [agency administrator], while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance. The weight of such a judgment in a particular case will depend upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control.").

[FN159]. Mead, 533 U.S. at 228 (footnotes omitted).


[FN161]. See id. at 125-26 (holding, in a 5-4 decision, that the Court would not defer to the FDA on the question of whether Congress meant to delegate the agency the power to regulate tobacco as a drug).

[FN162]. Id. at 159-60.

[FN163]. See id. at 126-27 (noting that the FDA rulemaking that produced the tobacco regulation followed the FDA's receipt of more than 700,000 public submissions, "more than 'at any other time in its history on any other subject'" (quoting Regulations Restricting the Sale and Distribution of Cigarettes, 61 Fed. Reg. 44,396, 44,418 (Aug. 28, 1996))). The dissent rejected the notion that relative political accountability between an executive agency and Congress made any difference in such a case. See id. at 190-91 (Breyer, J., dissenting) ("Insofar as the decision to regulate tobacco reflects the policy of an administration, it is a decision for which that administration, and those politically elected officials who support it, must (and will) take responsibility...I do not believe that an administrative agency decision of this magnitude—one that is important, conspicuous, and controversial—can escape the kind of public scrutiny that is essential in any democracy. And such a review will take place whether it is the Congress or the Executive Branch that makes the relevant decision.").


[FN165]. See Massachusetts v. EPA, 549 U.S. 497, 533-34 (2007) (finding the EPA's refusal to determine whether greenhouse gases cause climate change to be arbitrary and capricious).


[FN168]. Id. at 1163-66.

[FN169]. Id. at 1163-64 (quoting INS v. Abudu, 485 U.S. 94, 110 (1988)). As Justice Kennedy explained: "The Attorney General's decision to bar an alien who has participated in persecution 'may affect our relations with [the alien's native] country or its neighbors. The judiciary is not well positioned to shoulder primary responsibility for assessing the likelihood and importance of such diplomatic repercussions.'" Id. at 1164-65 (quoting INS v. Aguirre-Aguirre, 526 U.S. 415, 425 (1999)).

[FN170]. Id. at 1166.

[FN171]. Id.
[FN172]. Id. at 1167-68 (quoting Gonzalez v. Thomas, 547 U.S. 183, 186-87 (2006) (per curiam)). Indeed, Justice Kennedy noted “[t]hese matters may have relevance in determining whether its statutory interpretation is a permissible one.” Id.


[FN175]. See, e.g., 2 The Debates in the Several State Conventions on the Adoption of the Federal Constitution 350 (Jonathan Elliot ed., 1968) (“The true principle of government is this--make the system complete in its structure, give a perfect proportion and balance to its parts, and the powers you give it will never affect your security.” (quoting Alexander Hamilton)); The Federalist No. 47, at 324 (James Madison) (Jacob E. Cooke ed., 1961) (“The accumulation of all powers legislative, executive and judiciary in the same hands, whether of one, a few or many, and whether hereditary, self appointed, or elective, may justly be pronounced the very definition of tyranny.”); see also Mistretta v. United States, 488 U.S. 361, 380 (1989) (“This Court consistently has given voice to, and has reaffirmed, the central judgment of the Framers of the Constitution that, within our political scheme, the separation of governmental powers into three coordinate Branches is essential to the preservation of liberty.”); Gordon S. Wood, The Creation of the American Republic, 1776-1787, at 549 & n.42 (1998 ed.) (citing John Jay for the proposition that separation of powers could help avoid governmental tyranny). The unsupported assertion in Posner and Sunstein’s article that “critics and supporters agree that changes in the global environment justifying at least some expansion of executive powers,” Posner & Sunstein, supra note 3, at 1210, is particularly striking in this regard. See, for example, infra note 261 for articles by Kim Sheppele and Martin Flaherty taking the opposite view.

[FN176]. See Pearlstein, supra note 174, at 1592 (suggesting that detention regimes, for example, may benefit from multibranch participation).

[FN177]. Posner & Sunstein, supra note 3, at 1207.

[FN178]. Bradley, supra note 11, at 651.

[FN179]. See Deborah N. Pearlstein, Finding Effective Constraints on Executive Power: Interrogation, Detention, and Torture, 81 Ind. L.J. 1255, 1274-79 (2006) (describing the American military’s “professionalism”—that is, “the institutional acquisition and maintenance of a set of technical skills, norms, and ethics”--as a “defining feature”); Pearlstein, supra note 174, at 1608 (stating that organization theorists recognize the significant benefits of “strict bureaucratic control, intense socialization, and a highly developed sense of organizational culture” for government structures tasked with preventing high-consequence risk).


[FN181]. Posner & Sunstein, supra note 3, at 1214.
[FN182]. See id. at 1205 ("[T]he nature of the relationship with the foreign state, the cultural norms of that state, its legal system and other institutions, its politics, and so forth...are factors followed and assessed by the Department of State.").


[FN184]. Id. at 533–34 (citing Control of Emissions from New Highway Vehicles and Engines, 68 Fed. Reg. 52,922, 52,931 (Sept. 8, 2003)). The Court went on to reason,

       [EPA] has offered a laundry list of reasons not to regulate...Although we have neither the expertise nor the authority to evaluate these policy judgments, it is evident they...[do not] amount to a reasoned justification for declining to form a scientific judgment....In the Global Climate Protection Act of 1987, Congress authorized the State Department—not EPA—to formulate United States foreign policy with reference to environmental matters relating to climate. EPA has made no showing that it issued the ruling in question here after consultation with the State Department.

       Id.

[FN185]. See Neal Kumar Katyal, Hamdan v. Rumsfeld: The Legal Academy Goes to Practice, 120 Harv. L. Rev. 65, 105–06 (2006) (suggesting that the Hamdan Court might have appropriately deferred to the executive if the executive could have presented its interpretation "as the product of deliberative and sober bureaucratic decisionmaking").

[FN186]. See, e.g., United States v. Mead Corp., 533 U.S. 218, 228 (2001) (finding that courts have considered, among many factors, the agency's relative expertise and the "persuasiveness" of its position to decide what deference it deserves).


[FN188]. See, e.g., Mistretta v. United States, 488 U.S. 361, 421–22 (1989) (Scalia, J., dissenting) (arguing that the Court's holding that the United States Sentencing Commission does not upset separation of powers is an "undemocratic precedent" that could lead to further Congressional delegation of lawmaking to commissions that are not accountable to the political process); Morrison v. Olson, 487 U.S. 654, 731 (1988) (Scalia, J., dissenting) ("[T]he difference is the difference that the Founders envisioned when they established a single Chief Executive accountable to the people: the blame can be assigned to someone who can be punished.").

[FN189]. See Jinks & Katyal, supra note 3, at 1246 & n.58 (questioning the effectiveness of political accountability in the foreign affairs context); Pearlstein, supra note 174, at 1575–79 (noting that the government interest in secrecy surrounding some national security matters may make political checks on the executive that depend on transparency less effective).


[FN191]. Pearlstein, supra note 174, at 1578.

[FN192]. See, e.g., Farina, supra note 17, at 525 (noting tension between Chevron's deference regime and the judiciary's authority to determine statutory meaning).
[FN193]. See infra Part II.

[FN194]. Bradley, supra note 11, at 650 & n.2 ("[C]ommentators [who express the 'Marbury perspective'] typically frame [the issue of deference in foreign affairs cases] as a choice between two extremes: either the courts in foreign affairs cases enforce the 'rule of law' against the Executive or they abdicate their judicial function.") (citing, inter alia, Frack, supra note 38, at 4-5 (1992), and Harold Hongju Koh, The National Security Constitution: Sharing Power After the Iran-Contra Affair 148 (1990)); see also generally Alex Glashausser, Difference and Deference in Treaty Interpretation, 50 Vill. L. Rev. 25 (2005) (opposing deference to the executive's interpretation of treaties on formal grounds).


[FN196]. See, e.g., United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 320 (1936) (describing the President as the "sole organ of the federal government in the field of international relations").


[FN199]. See Monaghan, supra note 24 at 25-26 ("Judicial deference to agency 'interpretation' of law is simply one way of recognizing a delegation of law-making authority to an agency." (emphasis omitted)); see also United States v. Mead Corp., 533 U.S. 218, 226-27 (2001) ("[A]dministrative implementation of a particular statutory provision qualifies for Chevron deference when it appears that Congress delegated authority to the agency generally to make rules carrying the force of law...").

[FN200]. For example, in Whittman v. American Trucking Ass'n, the Court gave voice to delegation concerns in rejecting the notion that an agency could cure an unlawful delegation of legislative power by giving the statute a narrow construction. See 531 U.S. 457, 473 (2001) ("The very choice of which portion of the power to exercise—that is to say, the prescription of the standard that Congress had omitted—would itself be an exercise of the forbidden legislative authority. Whether the statute delegates legislative power is a question for the courts, and an agency's voluntary self-denial has no bearing upon the answer."). Beyond this, there seems broad agreement that nondelegation concerns continue to manifest themselves in interpretive canons against delegation. See infra note 238 (discussing the nondelegation canon). There also remain periodic signs elsewhere that the Court has retained an interest in policing formal structural constraints. Since Chevron, the Court has continued to produce decisions insisting that formal lines are drawn between and among the branches. See, e.g., Bowsher v. Synar, 478 U.S. 714, 732-34 (1986) (rejecting a statute through which Congress vested executive powers in an agency official but reserved for itself the power to remove him from office); INS v. Chadha, 462 U.S. 919, 959 (1983) (invalidating the so-called legislative veto of executive agency action).

[FN202]. 5 U.S. (1 Cranch) 137 (1803).

[FN203]. Id. at 177.

[FN204]. See id. at 165-66 ("By the constitution of the United States, the President is invested with certain important political powers, in the exercise of which he is to use his own discretion, and is accountable only to his country in his political character, and to his own conscience. To aid him in the performance of these duties, he is authorized to appoint certain officers, who act by his authority and in conformity with his orders. In such cases, their acts are his acts; and whatever opinion may be entertained of the manner in which executive discretion may be used, still there exists, and can exist, no power to control that discretion. The subjects are political. They respect the nation, not individual rights, and being entrusted to the executive, the decision of the executive is conclusive.").


[FN206]. See, e.g., John F. Duffy, Administrative Common Law in Judicial Review, 77 Tex. L. Rev. 113, 116 (1998) ("[L]egislators are the lawmakers... [and so] courts deciding statutory cases are bound to follow commands and policies embodied in the enacted text--commands and policies the courts did not create and cannot change."); Richard A. Posner, Legal Formalism, Legal Realism, and the Interpretation of Statutes and the Constitution, 37 Case W. Res. L. Rev. 179, 189 (1986) ("In our system of government the framers of statutes... are the superiors of the judges. The framers communicate orders to the judges through legislative texts....If the orders are clear, the judges must obey them."); Cass R. Sunstein, Interpreting Statutes in the Regulatory State, 103 Harv. L. Rev. 405, 415 (1989) ("According to the most prominent conception of the role of courts in statutory construction, judges are agents or servants of the legislature....The judicial task is to discern and apply a judgment made by others, most notably the legislature."); Nicholas S. Zeppos, Legislative History and the Interpretation of Statutes: Toward a Fact-Finding Model of Statutory Interpretation, 76 Va. L. Rev. 1295, 1313 (1990) ("Traditional democratic theory suggests that the court interpreting a statute must act as the faithful agent of the legislature's intent.").

[FN207]. See John F. Manning, Textualism and the Equity of the Statute, 101 Colum. L. Rev. 1, 85 (2001) (arguing that in debates leading up to the Constitution's ratification, the Federalists invoked the faithful agent notion to counter Anti-Federalist concerns).

[FN208]. Id. at 71.

[FN209]. Id. at 91 (quoting Schooner Paulina's Cargo v. United States, 11 U.S. (7 Cranch) 52, 60 (1812)).

[FN210]. Id. at 92.

[FN211]. Id. at 95-101.

[FN212]. Antonin Scalia, Assorted Canards of Contemporary Legal Analysis, 40 Case W. Res. L. Rev. 581, 583 (1990); see also John F. Manning, Lessons from a Nondelegation Canon, 83 Notre Dame L. Rev. 1541, 1553 (2008) ("A legislator who votes for...a provision...does so on the assumption that...what the words mean to him is identical to what they will mean to those to whom they are addressed."). (quoting Jeremy Waldron, Legislators' Intentions and Unintentional Legislation, in Law and Interpretation 329, 339 (Andrei Marmor ed., 1995)).

[FN213]. See Monaghan, supra note 24, at 60 ("Judicial deference to agency 'interpretation' of law is simply one way of recognizing a delegation of law-making authority to an agency.") (emphasis omitted)).
[FN214]. See William N. Eskridge, Jr., All About Words: Early Understandings of the “Judicial Power” in Statutory Interpretation, 1776-1806, 101 Colum. L. Rev. 990, 997 (2001) ("[T]he original materials surrounding Article III’s judicial power assume an eclectic approach to statutory interpretation, open to understanding the letter of a statute in pursuance of the spirit of the law and in light of fundamental values."); Molot, supra note 21, at 73 (suggesting that Chevron deference renders “[statutory] interpretation a political process”).

[FN215]. Faithful agent theory may be subject to attack on formal grounds as well, at least from those who conceive of the “executive power” in the foreign relations realm as carrying significant interpretive authority of its own. See, e.g., Sunstein, Beyond Marbury, supra note 11, at 2595 (suggesting that interpreting unclear terms in a foreign relations context may require deference to executive interpretation). This Article returns to such claims in Part III.


[FN217]. See supra notes 79-80 and accompanying text (discussing the Court’s focus on the interpretations of foreign treaty parties, in addition to those of the United States).

[FN218]. See Sullivan v. Kidd, 254 U.S. 433, 439 (1921) (“Writers of authority agree that treaties are to be interpreted upon the principles which govern the interpretation of contracts in writing between individuals...”).

[FN219]. See supra Section I.A (citing scholars advancing this view).


[FN221]. See supra note 78 and accompanying text.

[FN222]. See, e.g., Eskridge, supra note 21, at 117-18 (noting that the Framers expected judges both to “interpret statutes equitably” and to interpret statutes contrary to the legislature’s expectations, thereby requiring the legislature to examine the full impact of its enactments); Molot, supra note 21, at 3 & n.2 (describing the “instrumentalist” approach and citing scholarly analyses).

[FN223]. See Molot, supra note 21, at 34-38 (discussing the interpretive tools that the Framers believed were available to the judiciary to discern legislative intent).

[FN224]. Id. at 42.

[FN225]. According to Molot,

the prospect of judicial interpretation could provide just the ammunition that a legislator might need to defeat an unjust or irrational political compromise. A legislator might speak in opposition to a proposal that benefits one group at the expense of another, for example, not simply because the provision is unjust or irrational, but also because judges would likely construe the proposed provision more strictly than they would an alternative version that benefits both groups. Regardless of the individual legislator’s true motive, the judicial perspective would be wielded in favor of fairness and consistency in the legislative process.

Id. at 48 (footnote omitted). See also Molot, supra note 141, at 1301 (“[J]udges nonetheless strive for stability and consistency over time in a way that political officials do not.”).

[FN226]. Molot describes the judiciary’s role as follows:

When the judiciary draws boundaries between legislative enactments and executive leeway, it provides a benchmark for deliberation in the political process. It tells legislators what they must do to bind administrators and tells cit-
izens what they must do to comply with legislative instructions. By providing such a backdrop for public officials and private citizens, judicial interpretation tends to reinforce legislative authority and the rule of law.

Molot, supra note 141, at 1317.

[FN227]. See, e.g., John Hart Ely, War and Responsibility 54-56 (1993) (suggesting that the courts should induce Congress to check a presidential decision to go to war); Keh, supra note 194, at 123-32 (discussing congressional acquiescence to the executive's foreign policy initiatives in the wake of Cold War conflicts); Arthur M. Schlesinger, Jr., The Imperial Presidency 58-60 (1973) (chronicling the early erosion of the legislative check on executive war powers).

[FN228]. See U.S. Const. art. I, § 8 (giving Congress the power, inter alia, to declare war, define and punish offenses against the law of nations, and raise and support armies).

[FN229]. See Theodore J. Lowi & Benjamin Ginsberg, American Government: Freedom and Power 289-93 (1990) (describing the effects of executive action vis-à-vis foreign policy on presidential approval ratings); Theodore J. Lowi, The End of Liberalism 146 (2d ed. 1979) ("If the president can revive his major resource, his public following, with almost any international act with which he can clearly associate himself, then he must always be under some pressure to prefer such actions."). As Justice Jackson put it with characteristic eloquence:

I have no illusion that any decision by this Court can keep power in the hands of Congress if it is not wise and timely in meeting its problems. A crisis that challenges the President equally, or perhaps primarily, challenges Congress. If not good law, there was worldly wisdom in the maxim attributed to Napoleon that "the tools belong to the man who can use them." We may say that power to legislate for emergencies belongs in the hands of Congress, but only Congress itself can prevent power from slipping through its fingers.

Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 654 (1952) (Jackson, J., concurring).


[FN231]. See Hamdan v. Rumsfeld, 548 U.S. 557, 594-95 (2006) (stating that the Court's task was to determine whether presidential authorization of military commissions was justified).

[FN232]. See id. at 612-13 ("These simply are not the circumstances in which...a military commission established by Executive Order...may lawfully try a person and subject him to punishment.").


[FN235]. See Bradley & Goldsmith, supra note 23, at 2085-88 (noting that "[c]ourts often rely on past Executive Branch practice to inform the meaning of a federal statute").

[FN236]. See id. at 2085.

[FN237]. See William N. Eskridge, Jr., Interpreting Legislative Inaction, 87 Mich. L. Rev. 67, 91 (1988) ("For every case where the Court rhapsodizes about deliberative inaction, there is a counter-case subjecting such inferences to scathing critique. To explain the cause of non-action by Congress when Congress itself sheds no light is to venture into spec-
ulative unrealities'..." (quoting Helvering v. Hallock, 309 U.S. 106, 119-20 (1940)).

[FN238]. The nondelegation canon disfavors interpretations that would transfer significant swaths of discretionary power from one branch to another. Likewise, the canon of constitutional avoidance instructs the Court to disfavor readings that would threaten rights protected by the Constitution. Often invoked in the form of a clear statement requirement, such canons provide that the Court shall not construe a statute to infringe on constitutional rights or delegate significant power without a clear statement to that effect in the legal text. These canons may prove dispositive in resolving the meaning of a subconstitutional text. See Kenneth A. Bamberger, Normative Canons in the Review of Administrative Policymaking, 118 Yale L. J. 64, 79-80 (2008) (arguing that these canons allow courts to constrain congressional action).

[FN239]. A number of scholars have discussed the role of so-called normative canons in statutory interpretation. See, e.g., Eskridge & Frickey, supra note 22, at 598 ("A good many of the substantive canons of statutory construction are directly inspired by the Constitution..."); Sunstein, supra note 22, at 2111 ("By using these principles, courts decide cases of statutory meaning by reference to something external to legislative desires...").

[FN240]. See Bradley & Goldsmith, supra note 23, at 2103-06 (arguing against a clear statement requirement on delegation grounds in interpreting the AUMF).

[FN241]. The 1969 Vienna Convention on the Law of Treaties, setting forth detailed rules for the interpretation of treaties, has been ratified by 110 nations. See Vienna Convention on the Law of Treaties, supra note 20. The United States has signed but not ratified the treaty. Id. Nonetheless, the U.S. Department of State has on occasion acknowledged the Vienna Convention as "the authoritative guide to current treaty law and practice." Richard K. Gardiner, Treaty Interpretation 134 (2008) (quoting Cmmb & Son, Inc. v. Asiana Airlines, 214 F.3d 301, 308 (2d Cir. 2000)). The U.S. Supreme Court has not seemed much interested in the Vienna approach since the treaty entered into force in 1980. See id. at 133-38 (analyzing whether the Supreme Court's treaty-interpretation practice diverges from the Vienna rules).

[FN242]. See David Sloss, Judicial Deference to Executive Branch Treaty Interpretations: A Historical Perspective, 62 N.Y.U. Ann. Surv. Am. L. 497, 498-99 (2007) (noting that the U.S. government won less than twenty percent of cases between 1789 and 1838 in which a treaty was the basis of a claim or defense); see also supra subsection I.A.1 (reviewing multiple cases in which the Court asserted independent authority to interpret treaty obligations).

[FN243]. See, e.g., Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 473 (2001) ("The very choice of which portion of the power to exercise--that is to say, the prescription of the standard that Congress had omitted--would itself be an exercise of the forbidden legislative authority. Whether the statute delegates legislative power is a question for the courts, and an agency's voluntary self-denial has no bearing upon the answer."); Mistretta v. United States, 488 U.S. 361, 380 (1989) ("This Court consistently has given voice to, and has reaffirmed, the central judgment of the Framers of the Constitution that, within our political scheme, the separation of governmental powers into three coordinate Branches is essential to the preservation of liberty."); Duncan v. Kahanamoku, 327 U.S. 304, 322 (1946) ("Courts and their procedural safeguards are indispensable to the system of government. They were set up by our founders to protect the liberties they valued.").


[FN245]. See Monaghan, supra note 24, at 2 ("Marshall's grand conception of judicial autonomy in law declaration was not in terms or in logic limited to constitutional interpretation...").
[FN246]. See U.S. Const. art. III, § 2 ("The judicial Power shall extend to all Cases...arising under this Constitution, laws of the United States, and Treaties made...".


[FN249]. See Henkin, supra note 4, at 209 & nn.129-31 (describing the ability of legislation to supersede treaty provisions).

[FN250]. See supra Section II.B (discussing instrumental interpretation in further detail).

[FN251]. Farina, supra note 17, at 497 (quoting The Federalist No. 51, at 349 (James Madison) (Jacob E. Cooke ed., 1961)).

[FN252]. See id. at 487 ("[T]he Court's vision of separation of powers evolved...to the more flexible...proposition that power may be transferred so long as it will be adequately controlled.").

[FN253]. Id. at 497-98.

[FN254]. See, e.g., Kenneth A. Bamberger, Normative Canons in the Review of Administrative Policymaking, 118 Yale L.J. 64, 76 (2008) ("[S]hould statutory ambiguity be resolved by courts applying normative canons, as it was previous to Chevron? Or are these the kind of normative questions that should...be assigned to agency judgment?"); see also, e.g., Sunstein, supra note 230, at 315-16 (arguing that to the extent nondelegation doctrine remains of constitutional salience, it is enforced through the deployment of the interpretive canons). As noted previously, such canons have also been explained as a reasonable outgrowth of the faithful agent view of judicial power. See Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Const. Trades Council, 485 U.S. 568, 575 (1988) ("[T]he elementary rule is that every reasonable construction must be resorted to, in order to save a statute from unconstitutionality.' This approach not only reflects the prudential concern that constitutional issues not be needlessly confronted, but also recognizes that Congress, like this Court, is bound by and swears an oath to uphold the Constitution. The courts will therefore not lightly assume that Congress intended to infringe constitutionally protected liberties or usurp power constitutionally forbidden it." (quoting Hooper v. California, 155 U.S. 648, 657 (1895))).

[FN255]. See Bradley & Goldsmith, supra note 23, at 2102-06 (arguing that the Supreme Court has "made clear that delegation concerns are less significant when statutes concern foreign affairs than when they concern domestic affairs").
[FN256]. See Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 473 (2001) ("The very choice of which portion of the power to exercise—that is to say, the prescription of the standard that Congress had omitted—would itself be an exercise of the forbidden legislative authority. Whether the statute delegates legislative power is a question for the courts, and an agency's voluntary self-denial has no bearing upon the answer.").

[FN257]. Note that Bradley and Goldsmith reach the opposite conclusion on the relevance of the nondelegation canon to AUMF interpretation. See Bradley & Goldsmith, supra note 23, at 2102-06.

[FN258]. Medellin v. Texas, 552 U.S. 491, 523 (2008) (quoting Brief for United States as Amicus Curiae, supra note 5, at 5); see also supra subsection I.A.1 (discussing Medellin and related cases).

[FN259]. Medellin, 552 U.S. at 525 (quoting Brief for United States as Amicus Curiae, supra note 5, at 11) (emphasis omitted).

[FN260]. Id.

[FN261]. See, e.g., Martin S. Flaherty, Globalization and Executive Power 28 (Apr. 4, 2008) (unpublished manuscript) (on file with author) ("[G]lobalization generally has resulted in a net gain in power not for judiciaries, but for the "political" branches—and above all for executives -- within domestic legal systems."); Schepple, supra note 30, at 3-5 (describing how national executives have used a series of UN Security Council antiterrorism resolutions to expand executive power domestically).

[FN262]. 553 U.S. 674 (2008); see also supra subsection I.A.2 (discussing Munaf).

[FN263]. Munaf, 553 U.S. at 702.

[FN264]. Id.

[FN265]. See id. (finding that habeas petitioners had not successfully raised the claims in the lower courts). Petitioners had argued that transfer would violate their rights under a federal statute and treaty prohibiting the "return" of someone to another state when there is a substantial likelihood he will be tortured. Id. (citing Foreign Affairs Reform and Restructuring Act of 1998, Pub. L. No. 105-277, § 2242(a), 112 Stat. 2681-822, and Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, supra note 120).

[FN266]. See Pearlstein, supra note 174, at 1572 (arguing that while functional considerations may be relevant in separation-of-powers disputes, clear formal constraints remain important).


[FN269]. See Bradley & Goldsmith, supra note 23, at 2084 & n.150 (suggesting, inter alia, that the executive might be entitled to Chevron deference).

[FN270]. Id. at 2100-06.

[FN271]. Id. at 2100-01 (emphasis added) (quoting Loving v. United States, 517 U.S. 748, 772 (1996)).

[FN272]. Id. at 2103-04.
[FN273]. Id.


[FN276]. Id. at 4.

[FN277]. Id. at 11.

[FN278]. Id. at 17.

[FN279]. The other cases in the “passport trilogy,” relied on heavily by Bradley and Goldsmith, are likewise unhelpful in advancing the claim that the President's independent constitutional authority has some particular bearing on the Court's role in interpreting foreign relations statutes. In Kent v. Dulles, the Court held that statutes providing that passports may be issued under “such rules as President shall...prescribe” did not afford the executive the authority it claimed—namely, the power to deny passports to citizens who appeared to support the Communist Party. 357 U.S. 116, 123, 129 (1958); see also Bradley & Goldsmith, supra note 23, at 2101 (noting that the Kent Court declined to address whether a different analysis would be appropriate if the case had arisen during a war emergency). To the extent one might discern anything about what difference wartime (and therefore “war powers”) might have made in the Court’s reasoning, it was a difference regarding the treatment of individual rights, not the relative scope of Congress’s power to delegate authority or the executive’s power to exercise it. See Kent, 357 U.S. at 128 (distinguishing the instant case from the Court's wartime holding in Korematsu v. United States, 323 U.S. 214 (1944), on the grounds that “[n]o such showing of extremity, no such showing of joint action by the Chief Executive and the Congress to curtail a constitutional right of the citizen has been made here”). In contrast, in Haig v. Agee, 453 U.S. 280, 306 (1981), the Court did uphold the President’s delegated authority to revoke a passport on the ground that the holder’s activities abroad were causing serious harm to U.S. foreign policy. But there, the Court squarely foreclosed the possibility that its delegation analysis was based on an assessment of the President’s Article II powers. See Haig, 453 U.S. at 289 n.17 (“[W]e have no occasion in this case to determine the scope of ‘the very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations—a power which does not require as a basis for its exercise an act of Congress, but which, of course, like every other governmental power, must be exercised in subordination to the applicable provisions of the Constitution.’” (quoting United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 320 (1936))). Rather, the Court’s decision was based on a finding that Congress was aware of and, by taking no action over time, implicitly authorized a consistent executive branch practice of denying passports on such grounds. Haig, 453 U.S. at 302-03.

[FN280]. Loving v. United States, 517 U.S. 748 (1996), the key case Bradley and Goldsmith cite for this proposition, did not purport to establish a principle of delegation in foreign relations law in general. Rather, the case was narrowly limited to the Court’s understanding of the Commander-in-Chief function as including the particular responsibility to take “action to superintend the military...a specialized community governed by a separate discipline from that of the civilian.” Id. at 772-73 (quoting Orloff v. Willoughby, 345 U.S. 83, 94 (1953)).

[FN281]. See Sunstein, supra note 230, at 315-16 (arguing that nondelegation doctrine is “alive and well” in the form of substantive interpretive canons against delegation).

[FN283]. Whittington, supra note 247, at 782-83.

[FN284]. See generally Paulsen, supra note 248 (surveying such arguments in favor of the President's interpretive authority).

[FN285]. Kramer, supra note 248, at 31 (noting that communities once had a “credible interpretive voice when it came to the constitution”).

[FN286]. Pillard, supra note 248, at 687 (emphasis added) (footnote omitted).

[FN287]. Some departmentalists have pointed to the presidential oath of office, for example, as a textual basis for understanding the President as having some independent constitutional responsibility to explain (in service of upholding) the Constitution. That Clause imposes upon the President the duty to “preserve, protect and defend the Constitution of the United States,” not the Constitution, laws, and treaties of the United States. U.S. Const. art. II, § 1 (emphasis added); see also Laurence H. Tribe, American Constitutional Law 266-67 (3d ed. 2000) (recognizing the importance of the Oath Clause in the departmentalist argument). Other scholars have likewise made arguments grounded in political theory that are tied specifically to the task of constitutional interpretation. See, e.g., Kramer, supra note 248, at 106-10 (discussing how the three branches of government should reach compromise when their interpretations differ); Tushnet, supra note 248, at 6-32 (raising various arguments against judicial supremacy in constitutional interpretation).

[FN288]. While the Oath Clause may make executive interpretive authority over the Constitution of special significance, the Take Care Clause makes no such textual distinction between different sources of federal law. See U.S. Const. art. II, § 3 (“He shall take Care that the Laws be faithfully executed...”).

[FN289]. See Paulsen, supra note 248, at 222 (“The framers believed that liberty is best preserved where governmental power is diffused....”).

[FN290]. See, e.g., id. at 221 (“The Supreme Court's interpretations of treaties, federal statutes, or the Constitution do not bind the President any more than the President's or Congress's interpretations bind the courts.”); see also Dawn E. Johnsen, Functional Departmentalism and Nonjudicial Interpretation: Who Determines Constitutional Meaning?, Law & Contemp. Probs., Summer 2004, at 105, 113 (“All three branches share the responsibility to uphold the Constitution.”).

[FN291]. U.S. Const. art. III, § 2 (“The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority....”).


[FN293]. See U.S. Const. art. III (establishing the structure and jurisdiction of the federal courts).

[FN294]. Walter Dellinger and H. Jefferson Powell give an example of this concern:

In 1800, Congressman Marshall explained to the House of Representatives that the Constitution does not vest in the federal courts the exclusive authority to decide issues arising under the Constitution, laws and treaties; while such issues are by definition questions of law, some of them are “questions of political law,” and must be answered by one (or both) of the political branches of the government.


[FN296]. See Whittington, supra note 205, at 14 (describing a theory of "fixed departmentalism" that holds that "allocation of interpretive authority varies by topic or constitutional provision" (quoting Scott E. Gant, Judicial Supremacy and Nonjudicial Interpretation of the Constitution, 24 Hastings Const. L.Q. 359, 384 (1997))).

[FN297]. See Johnsen, supra note 290, at 112 (noting that a few departmentalists argue that the President should choose not to enforce laws if he finds them "constitutionally objectionable").

[FN298]. See Paulsen, supra note 248, at 222 (arguing that the President "may refuse to execute (or, where directed specifically to him, refuse to obey) judicial decrees that he concludes are contrary to law").


[FN300]. See John Yoo, Politics as Law?: The Anti-Ballistic Missile Treaty, the Separation of Powers, and Treaty Interpretation, 89 Calif. L. Rev. 851, 869-70 (2001) (book review) (contending that the Constitution imparts full control over treaty interpretation to the President). Although Yoo's position is set forth in the context of treaty interpretation specifically, his textual reading of Article II's Vesting Clause would appear to have implications for statutory interpretation as well. See also Bradley, supra note 11, at 699 (arguing that because the executive has broad constitutional authority of its own with regard to foreign affairs law, there should be little concern that shared authority—even shared interpretive authority—runs afoul of formal constitutional limits).

[FN301]. For example, Martin Flaherty highlights the historical deficiencies of Yoo's argument:

"The framers were virtually of one mind when it came to giving treaties the status of law.... The imperative need to make treaties legally binding on both the states and their citizens was widely recognized by 1787. The major consequence of this perception was the ready adoption of the supremacy clause, which gave treaties the status of law and made them judicially enforceable through the federal courts."


[FN302]. See U.S. Const. art. II, § 2 ("He shall have Power...to make Treaties, provided two thirds of the Senators present concur.....").

[FN303]. Id. art. III, § 2 (emphasis added).

[FN304]. See supra subsection I.A.1 (reviewing treaty-interpretation cases).
159 U. Pa. L. Rev. 783

END OF DOCUMENT
ARTICLES

NATIONAL SECURITY FACT DEERENCE

Robert M. Chesney*

I. NATIONAL SECURITY FACT DEERENCE IN PRACTICE ........ 1366
   A. Individual Eligibility for Military Detention .......... 1366
   B. Group Compliance with the Law of War ............... 1371
   C. The State Secrets Privilege ........................... 1376
   D. Military Exigency and Preparedness ................. 1380

II. THE NATURE OF A FACT DEERENCE CLAIM ............ 1385
   A. Fact Deference as a Decision Rule (Constitutional or
      Otherwise) ............................................. 1386
   B. Decision Rule Formation and the Issue of Relevant
      Considerations .......................................... 1392
      1. Core Accuracy ....................................... 1392
      2. Weighted Accuracy ................................. 1395
      3. Prudence ............................................ 1396
      4. Legitimacy ......................................... 1398

III. OBJECTIONS .................................................. 1400
    A. Window Dressing Objections ........................... 1400
    B. Definitional Objections to "National Security" .... 1402

IV. TESTING THE JUSTIFICATIONS FOR NATIONAL SECURITY
    FACT DEERENCE ........................................ 1403
    A. Core Accuracy and Comparative Institutional
       Competence ............................................ 1404

* Professor, University of Texas School of Law. I am grateful to Mitch Berman, Richard Fallon, Paul Horowitz, Jide Nzelibe, Deborah Pearlstein, Michael Ramsey, Ed Richards, Matthew Waxman, Christina Wells, Ron Wright, and participants in faculty workshops at the University of Texas, Louisiana State University, and Southwestern for helpful criticisms and suggestions.

1361
SHOULD judges defer to factual judgments made by the executive branch in litigation involving national security? The executive branch frequently argues that judges should do precisely that, and though courts often express reservations, they often comply in the end.

This practice—what I will refer to as “national security fact deference”—is freighted with constitutional significance. On one hand, it may undermine the capacity of courts to guard against unlawful executive branch actions (in terms of both unjustified assertions of power and violations of individual rights). On the other hand, it may prevent the judicial power from encroaching inappropriately upon executive responsibilities relating to national security, while simultaneously helping to preserve the judiciary’s institutional legitimacy. National security fact deference claims, in short, implicate competing values of great magnitude.

How courts resolve this tension says much about our constitutional order in an age of increasingly ubiquitous national security concerns, yet the practice of fact deference is not widely recognized or studied. Courts and commentators have, of course, long grappled with a variety of related deference concepts.¹ Too little atten-

tion has been paid, however, to the distinct issues that arise when courts deem national security disputes justiciable and the executive branch then falls back on the position that courts at least should defer to its factual judgments. I aim to close that gap in this article by developing an account of the nature of national security fact deference claims and, in light of that account, by conducting a probing review of the considerations that might be cited in favor of a deference obligation. Ultimately, I conclude that many arguments in favor of deference are unpersuasive, but that deference nonetheless may be justified in limited circumstances.

Part I opens with a descriptive account of how national security fact deference claims have been litigated and resolved in actual practice. This serves several purposes. First, it illustrates the transsubstantive nature of this practice, with examples ranging from enemy combatant status litigation to environmental suits challenging the Navy’s use of sonar during training exercises. Second, the survey demonstrates the significance of national security fact deference claims in terms of individual cases, showing that they can have a dispositive impact on the merits. Finally, and most significantly, it suggests that national security fact deference claims are plagued by doctrinal and theoretical confusion, with courts and litigants alike


uncertain as to which considerations should govern and how if at all they ought to be balanced against one another.

Against that backdrop, Part II develops an account of the nature of national security fact deference claims. I suggest that such claims are best understood as a species of "decision rule." This account, which I derive from the literature of constitutional theory, emphasizes the distinction between the abstract meaning of a legal rule and the practical need to develop an implementation framework—that is to say, decision rules—that will permit a judge to bring that meaning to bear in the particular institutional context of litigation. At a minimum, for example, a judge cannot avoid adopting some standard of proof in the course of determining whether the constituent elements of a legal rule have been satisfied or violated. Where another institution already has made a judgment regarding those predicate questions, the judge also must determine whether to defer to that judgment. From this point of view, resolving a deference claim is a paradigmatic example of decision rule formation.

Viewing national security fact deference claims through the lens of the decision rules literature has practical benefits in terms of identifying and analyzing the considerations that may be relevant to resolving such claims. For present purposes, the most relevant of these considerations can be grouped under four headings. The first is core accuracy, a term that describes the goal of minimizing the net amount of false positives and false negatives generated in the course of implementing the underlying legal rule. This contrasts with the second, weighted accuracy, which considers the possibility that there may be individualized or systemic reasons to prefer more false positives than false negatives in a particular setting, or vice versa. The third, prudential concerns, includes the efficiency of the decision-making process in terms of speed or resource consumption, the potential collateral impact that resolution of the deference question may have on related government activities such as ongoing combat operations or the maintenance of secrecy, the judiciary's instinct for self-preservation in light of the risk of political blowback, and the prospect that another institution is better suited to exercise final judgment in light of its superior democratic accountability. Finally, formal legitimacy claims involve the concern that the law vests decisionmaking authority in another institution.
Before proceeding to a close analysis of how these justifications may or may not apply in the context of fact deference claims in national security litigation, Part III pauses to address potential objections to this project. One might object, for example, that judicial analysis of these factors constitutes mere window dressing, and that these claims actually turn on the judge’s policy or value preferences. And even if one accepts that legal factors play a meaningful role in resolving fact deference claims as a general proposition, one might still object to the notion that the vague concept “national security” will play a substantive role in the analysis. These are serious concerns, to be sure, and they remind us of the need to proceed with great care and nuance in discussing the criteria relevant to resolving fact deference claims. They do not, however, require us to abandon that inquiry altogether.

Part IV is the heart of my analysis. In it, I parse the arguments identified in Part II in order to determine what insights they may yield regarding the resolution of national security fact deference claims. Because these considerations for the most part are sensitive to the circumstances of particular cases, we cannot and should not pursue a one-size-fits-all model for resolving fact deference claims. Nonetheless, the exercise produces a set of observations that collectively can do much to improve the coherence and defensibility of national security fact deference claims. For example, the analysis suggests that fact deference claims primarily turn on comparative institutional accuracy concerns, along with concerns about democratic accountability and institutional self-preservation; that judges conducting comparative accuracy inquiries must account separately for the possibility that the executive has superior access to information and to expertise, and should require a showing that the executive actually and reliably exploited such advantages; that arguments regarding the relative strength of the governmental, private, and social interests at stake in national security litigation frequently will be indeterminate, thus undermining the case for weighting the comparative accuracy inquiry so as to encourage false positives or false negatives; that efficiency and secrecy concerns are better addressed through doctrinal mechanisms other than fact deference; and that arguments involving comparative institutional legitimacy, though quite common, do little or no sepa-
rate work once one accounts for comparative accuracy, democratic accountability, and institutional self-preservation.

These guidelines and insights are unlikely to please either ardent supporters or critics of national security fact deference. They tend to exclude fact deference as unjustifiable in many circumstances, while providing support for it in others. And they certainly do not entirely eliminate disagreement and uncertainty when such claims arise. Indeed, much room for debate and discretion remains. Nonetheless, there is substantial benefit to be had in debunking some of the arguments that arise in this setting and insisting upon a more nuanced and defensible approach to the others.

I. NATIONAL SECURITY FACT DEFERENCE IN PRACTICE

National security fact deference claims arise across an array of doctrinal settings, often with dispositive effect. Unfortunately, a review of how such claims have been addressed in actual practice suggests that litigants and judges lack a shared understanding of the nature of such claims and of the arguments that are relevant to resolving them.¹

In the pages that follow, I review the actual practice of national security fact deference by surveying four distinct contexts in which such claims have arisen. These scenarios involve determinations of whether a person was properly classified as an enemy combatant, whether federal criminal charges against an alleged Taliban member should be dismissed on grounds of combatant immunity, whether public disclosure of classified information would harm national security, and whether certain conduct would harm military preparedness. In each setting, litigants and judges have struggled to determine whether and to what extent deference might be warranted.

A. Individual Eligibility for Military Detention

Perhaps the most widely appreciated example of national security fact deference in the post-9/11 era involves the attempt by the government—ultimately unsuccessful—to persuade courts to defer

¹ Paul Horwitz recently observed that such under-theorization is a problem more generally for deference as a "transsubstantive tool of constitutional law." Paul Horwitz, Three Faces of Deference, 83 Notre Dame L. Rev. 1061, 1066 (2008).
to its judgment that specific individuals have engaged in conduct warranting military detention as enemy combatants.

The case that best illustrates this involved an American citizen named Yaser Hamdi, thought by the government to have fought for the Taliban. The U.S. military took custody of Hamdi in Afghanistan in the fall of 2001, later sending him to Guantánamo and then, after learning of his citizenship, to a military detention facility in the United States. The government initially argued that Hamdi's habeas petition was not justiciable at all because of his status as a military prisoner. As a fallback position, however, the government also argued that the courts should at least defer to its factual judgment regarding Hamdi's past conduct.

The government offered an array of arguments in support of its deference claim. First, it claimed that separation of powers required deference in this setting, citing the textual allocation to the executive of the commander-in-chief function as well as the Supreme Court's 1936 determination in United States v. Curtiss-Wright Export Corp. that the president is the "sole organ" of the government in foreign affairs. Second, it offered prudential and functional arguments: failure to defer would harm ongoing military operations by diverting the attention (or even the physical presence) of commanders in the field; and, in any event, courts lacked the expertise to review questions of enemy combatant

---

4 The role of fact deference in this setting has been obscured by debate regarding federal court habeas jurisdiction over Guantánamo detainees. See Boumediene v. Bush, 128 S. Ct. 2229 (2008).
7 See id. at 13.
8 Here I use "functional" in the sense that Deborah Pearlstein describes as "effectiveness functionalism." See Deborah N. Pearlstein, Form and Function in the National Security Constitution, 41 Conn. L. Rev. (forthcoming July 2009), available at http://ssrn.com/abstract=1159595, at 6 (describing "purposive" functionalism as the pursuit of arrangements that best serve a larger constitutional goal and "effectiveness" functionalism as the pursuit of "immediate issues of effectiveness, efficiency, and the circumstantial needs of modern government").
9 See Brief for Respondents-Appellants, supra note 6, at 15–16 (citing Johnson v. Eisentrager, 339 U.S. 763, 779 (1950)).
The government acknowledged that deference, if binding, would preclude the judiciary from acting as much of a check against executive branch abuse, but it argued that when it came to misuse of military power the "Founders" had expected such concerns to be addressed at the ballot box rather than through litigation.11

The United States Court of Appeals for the Fourth Circuit agreed, placing a particular emphasis on functional concerns.12 "The executive is best prepared to exercise the military judgment attending the capture of alleged combatants," the panel held, adding that judicial review of detention decisions "must not present a risk of saddling military decision-making with the panoply of encumbrances associated with civil litigation," and warning that "development of facts may pose special hazards of judicial involvement in military decision-making."13 Yet the court was unwilling to treat the executive's determination as entirely binding given that the liberty of a citizen was at stake.14 Instead, the Fourth Circuit directed the district court to develop a procedure on remand that would show appropriate deference to the executive's position—whatever that might mean in practical terms—in light of these considerations.15

The government at that point sought to satisfy judicial review of Hamdi's detention by providing a two-page declaration summarizing the circumstances in which Hamdi had been captured and the process by which he had been classified as an enemy combatant.16

---

10 Id. at 30 ("Not only do courts lack the expertise to evaluate military tactics, but they will often be without knowledge of the facts and standards upon which military decisions have been based.") (quoting Tiffany v. United States, 931 F.2d 271, 278 (4th Cir. 1991)).

11 The government relied upon an earlier decision of the Fourth Circuit that had itself relied upon Federalist No. 26 for the proposition that "if the majority should be really disposed to exceed the proper limits, the community will be warned of the danger [by the minority], and [the community] will have an opportunity of taking measures to guard against it," and Federalist No. 78 for the notion that the Judiciary has "no influence over either the sword or the purse." See id. at 32 (citing Thomasson v. Perry, 80 F.3d 915, 924 (4th Cir. 1996)).


13 Id. at 283–84.

14 See id. at 283.

15 See id. at 283–84.

The United States District Court for the Eastern District of Virginia found this inadequate, stressing the need to ensure that deference not become dispositive where individual rights are at stake. The Fourth Circuit reversed, however, again emphasizing functional concerns: the executive wields the relevant "expertise and experience," the panel wrote, and "courts are ill-positioned to police the military's distinction between those in the arena of combat who should be detained and those who should not." Accordingly, the Fourth Circuit held that

no evidentiary hearing or factual inquiry on our part is necessary or proper, because it is undisputed that Hamdi was captured in a zone of active combat operations in a foreign country and because any inquiry must be circumscribed to avoid encroachment into the military affairs entrusted to the executive branch.

These well rehearsed arguments next moved to the Supreme Court of the United States, which charted a middle course in a splintered opinion. A plurality rejected the government's position, giving little regard to the executive's claim of functional advantages and concluding that separation of powers concerns forbade binding deference. Nevertheless, the plurality was sensitive to the pruden-

---

17 See id. at 532–36.
18 Hamdi v. Rumsfeld, 316 F.3d 450, 463, 474 (4th Cir. 2003). The court also noted prudential concerns regarding disruption of military operations. See id. at 465–66 (citing risk of commanders being called into court from the field); id. at 471 (citing impact on military "efficiency and morale," and the sheer logistical difficulties involved in trying "to acquire evidence from far away battle zones"); id. at 474 (same).
19 Id. at 473.
20 See Brief for Petitioners at 21–26, Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696) (arguing that deference undermined separation of powers values by emasculating judicial review of executive detention authority); Brief for the Respondents at 25–27, Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696) (arguing that eligibility for detention is a military judgment exclusively allocated to the executive branch, that the executive has superior competence to make such judgments, and that the judiciary lacks the political accountability that ought to attend such determinations).
21 Hamdi v. Rumsfeld 542 U.S. 507, 528–32 (2004) (citing judicial review as a check on the risk of executive abuse, but also noting that "core strategic matters of wargaming belong in the hands of those who are best positioned and most politically accountable for making them" and that judicial inquiry into the facts not only runs a risk of disrupting the war effort but also may prove to be in vain).
22 See id. at 535–36 (holding that "we necessarily reject the Government's assertion that separation of powers principles mandate a heavily circumscribed role for the courts in such circumstances. Indeed, the position that the courts must forgo any ex-
tial concerns the government had raised, especially the prospect that review might impose difficult logistical burdens on the government that could interfere with ongoing military operations.23

"With due recognition of these competing concerns," Justice O'Connor concluded, "we believe that neither the process proposed by the Government nor the process apparently envisioned by the District Court below strikes the proper constitutional balance . . . "24 Instead, she called for the government to provide Hamdi with a "fair opportunity to rebut the Government's factual assertions before a neutral decisionmaker,"25 while also endorsing procedural measures designed to ameliorate the collateral burdens potentially imposed by such review, including the use of hearsay evidence or even a presumption of accuracy for the government's evidence.26

Taken as a whole, the Hamdi litigation suggests a lack of consensus regarding the role that certain types of arguments should play in resolving fact deference claims. Most if not all the judges were mindful to at least some degree of the prudential concerns associated with the potential impact of litigation on the ongoing conduct of military operations, but beyond this, agreement broke down. The Fourth Circuit judges placed considerable weight on functional claims relating to the asserted competence advantage of the

23 See id. at 534–35.
24 Id. at 532.
25 Id. at 533.
26 See id. at 533–34. Only Justice Thomas wrote to support the government's position on deference. See id. at 579 (Thomas, J., dissenting) ("This detention falls squarely within the Federal Government's war powers, and we lack the expertise and capacity to second-guess that decision."). Justice Thomas argued that courts lack the information available to the executive branch and that "even if the courts could compel the Executive to produce the necessary information, such decisions are simply not amenable to judicial determination because "[t]hey are delicate, complex, and involve large elements of prophecy."" Id. at 583 (quoting Chicago & S. Air Lines v. Waterman S.S. Corp, 333 U.S. 103, 111 (1948) (calling for deference to Presidential judgments regarding diplomatic consequences of granting a license for international air travel)).
executive branch, but the Supreme Court plurality gave little regard to that consideration. Some of the judges and Justices thought that it mattered a great deal that constitutional rights were at stake, others appeared not to account for this. And though most of the Justices were uninterested in formalist arguments to the effect that deference should follow from the Constitution’s allocation of certain national security and foreign affairs responsibilities to the executive branch, at least one thought this quite important.\(^7\)

**B. Group Compliance with the Law of War**

Many of the themes developed in *Hamdi* also were on display in the litigation involving Hamdi’s fellow “American Taliban,” John Walker Lindh. In Lindh’s case, however, the dispute did not concern his own past conduct but, rather, the collective past conduct of the Taliban itself.

Unlike Hamdi, the government did not hold Lindh as an enemy combatant. Instead, it charged him with an array of federal crimes stemming from his involvement with the Taliban. Lindh subsequently moved to dismiss the indictment, arguing among other things that he was entitled to the affirmative defense of combat immunity.\(^8\) "Combat immunity" prohibits a state from applying its domestic criminal law to the actions of an enemy soldier so long as those actions did not violate the law of war.\(^9\) To claim it, the person must have qualified at the time of the conduct in question as a privileged belligerent under the law of war.\(^10\) According to Lindh, the test for privileged belligerency in turn depends on whether a

---

\(^7\) See id. at 580 (Thomas, J., dissenting) (arguing that the Founders intended for the President to have primary responsibility for national security affairs).

\(^8\) See Memorandum of Points and Authorities in Support of Motion to Dismiss Count One of the Indictment for Failure to State a Violation of the Charging Statute (Combat Immunity) (Motion #2), United States v. Lindh, Crim. No. 02-37-A [E.D. Va. 2002] [hereinafter Lindh Memorandum].

\(^9\) See Waldemar A. Solf & Edward R. Cummings, A Survey of Penal Sanctions Under Protocol I to the Geneva Conventions of August 12, 1949, 9 Case W. Res. J. Int’l L. 205, 212 (1977) (“[T]hose who are entitled to the juridical status of ‘privileged combatant’ are immune from criminal prosecution for those warlike acts which do not violate the laws and customs of war but which might otherwise be common crimes under municipal law.”).

\(^10\) See id. at 212–13.
person would qualify for prisoner-of-war (POW) status if captured.\textsuperscript{31} Article 4 of the Geneva Convention (III) Relative to the Treatment of Prisoners of War (GPW) specifies several circumstances under which a person detained in connection with an international armed conflict should be categorized as a POW.\textsuperscript{32} Article 4(A)(1), for example, extends POW status to the members of the "armed forces" of a party to the conflict, and Article 4(A)(3) clarifies that this rule applies irrespective of whether the detaining power recognizes that party as a government. Article 4(A)(2) extends POW status beyond the members of the armed forces proper, moreover, to members of militias and volunteer corps that fight on behalf of a party,

provided that such militias or volunteer corps, including such organized resistance movements, fulfil [sic] the following conditions: (a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; [and] (d) that of conducting their operations in accordance with the laws and customs of war.\textsuperscript{33}

Lindh invoked all three categories recognized under Article 4 in support of his combat immunity defense.\textsuperscript{34} He faced a significant hurdle, however, in that President Bush in February 2002 had issued an order concluding that Taliban fighters collectively failed to

\textsuperscript{31} See Lindh Memorandum, supra note 28, at 14–15; Memorandum Amicus Curiae Opposing Recognition of ‘Combat Immunity’ for Defendant Lindh in Regard to his Armed Support of Terrorism, United States v. Lindh, Crim. No. 02-37-A, at 6–11 (E.D. Va. 2002), available at http://fedsoc.server326.com/pdf/lindh.pdf (endorse this interpretation of the elements of the test, but coming to a different conclusion regarding whether the test was satisfied in this instance).

\textsuperscript{32} POW status, according to GPW, is available only in connection with an international armed conflict as that phrase is defined in Common Article 2 of the Geneva Conventions. Geneva Convention Relative to the Treatment of Prisoners of War art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 3318.

\textsuperscript{33} Geneva Convention Relative to the Treatment of Prisoners of War art. 4, Aug. 12, 1949, 6 U.S.T. 3316, 3320.

qualify for POW status under any category. The reasoning underlying the President’s determination can be gleaned from the Department of Justice memoranda that informed the decision. In relevant part, these documents advanced a three-step argument. First, the conditions of lawful belligerency specified in Article 4(A)(2) apply equally to POW status claims under Articles 4(A)(1) and (3). Second, compliance with those conditions can be determined at the collective rather than at the individual level. And third, the available evidence suggests that the Taliban collectively failed to satisfy any of the four conditions. The first two steps in this argument constitute treaty interpretations and hence are beyond the scope of this article, though they are important and controversial conclusions that warrant further attention. The third step, in contrast, involved factfinding.

As happened in Hamdi, the government in Lindh responded with both a political question argument and a fact deference argu-

37 See, e.g., Bybee Jan. 22 Memo, supra note 36, at 90.
38 For a review of the debate concerning extension of the four conditions to Articles 4(A)(1) and (3) despite the fact that they appear in the text only of Article 4(A)(2), see Robert M. Chesney, Leaving Guantánamo: The Law of International Detainee Transfers, 40 U. Rich. L. Rev. 657, 718–28 (2006). On the question of collective versus individual compliance, see id. at 728–29; Rona, supra note 34, at 717 (stating that “reasonable scholars differ over whether [noncompliance] . . . disqualifies just the individuals who commit [war crimes] or the entire entity of which they are a part”).
39 See Bybee Feb. 7 Memo, supra note 36, at 2–4; Memorandum from John Yoo and Robert J. Delahunt, supra note 36, at 62; Bybee Jan. 22 Memo, supra note 36, at 101.
First, the government argued that the president’s order was “not subject to review in this Court” because it constituted a “non-justiciable political question” that “conclusively forecloses any claim that the defendant could have combatant immunity by virtue of membership in the Taliban militia.” Second, the government argued that the president’s judgment, even if justiciable, “would still be entitled to great deference simply because it involves the interpretation and application of a treaty—the GPW.”

At first glance, the political question argument appeared to rest on a formal legitimacy claim that specification of the legal status of the enemy under the laws of war belongs exclusively to the executive branch under the rubric of the President’s commander-in-chief and foreign affairs powers. On closer inspection, however, the claim reduces to a functional argument emphasizing comparative institutional competence. The government explained that questions involving war and foreign affairs are “of a kind for which the Judiciary has neither aptitude, facilities nor responsibility.” This is particularly true with respect to the Taliban’s compliance with the four conditions for lawful belligerency, the government argued, since the President has superior access to information on these subjects. “Courts, indeed, are singularly ill-equipped to make factual findings about conditions in an area of active combat operations,” the government warned. “While the President has available multiple sources of information and intelligence about organization

---

42 See Government’s Opposition to Defendant’s Motion to Dismiss Count One of the Indictment for Failure to State a Violation of the Charging Statute (Combat Immunity) (#2) at 2–3, 12, United States v. Lindh, Crim. No. 02-37-A (E.D. Va. 2002).
43 Id. at 2–3.
44 Id. at 12 (emphasis added).
45 Id. at 2; see also id. at 6–7 (contending that the “status of an armed group” under international humanitarian law “is a question committed exclusively to the President as Commander in Chief” because it “bears directly upon the President’s core constitutional authority to conduct military operations in defense of the Nation”); id. at 11 (“Military questions such as those involving the status of an armed group under the laws of war are ‘textually… committed’ by the Constitution to the political branches.”) (quoting Baker v. Carr, 369 U.S. 186, 217 (1961)).
46 Id. at 9 (internal quotation marks and citations omitted).
47 Id. at 11 (quoting United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936) (observing that the President “has the better opportunity of knowing the conditions which prevail in foreign countries, and especially is this true in time of war”)).
2009] National Security Fact Deference 1375

and structure of forces opposing the United States," for example, "this Court is hardly well equipped to undertake that inquiry."

The government had much less to say in support of its alternative argument that the court should at least afford "great deference" to the President's determination even if it is not entirely binding. What it did have to say, however, illustrates the confusion that often plagues the doctrinal manifestation of deference principles. The government might have rested this argument on the very same considerations cited above, reasoning that they afford prudential grounds for caution even if they do not support application of the political question doctrine. But it did not do so. Rather, it pointed out that the President's determination arose against the backdrop of treaty law, and that there is a doctrine calling for courts to defer to the President's interpretation of ambiguous treaty language. But determining whether the Taliban complied with the Article 4(A)(2) conditions is a factfinding question. The treaty deference cases simply do not speak to this scenario.

The district court ultimately balked at the suggestion that it was bound by the President's resolution of the factual issues raised by Lindh's claim to POW status. Faced with the government's institutional legitimacy and comparative competence arguments, the court countered that "it is central to the rule of law in our constitutional system that federal courts must, in appropriate circumstances, review or second guess, and indeed sometimes even trump, the actions of the other governmental branches." But it is one thing to insist that there must be some form of judicial review, and quite another to say that such review must be non-deferential.

Having laid down a symbolic marker for judicial independence by rejecting the government's invocation of the political question doctrine, the court proceeded to conclude that the President's fac-

---

49 Id. at 19; see also id. at 20 (arguing that courts lack capacity to resolve fact disputes regarding issues such as "the extent of systematic organization and hierarchical command within an armed faction in a distant land"); id. at 23 ("The President has available far superior sources of intelligence and information for evaluating the conduct of a foreign force that poses a military threat to the Nation . . . .").

50 See id. at 12–14 (citing, inter alia, United States v. Stuart, 489 U.S. 353, 369 (1989)).


52 Id.
tual determination nonetheless deserved substantial deference.\textsuperscript{51} The court first referred to the same inapposite treaty interpretation principles noted above, asserting without citation that “deference here is appropriately accorded not only to the President’s interpretation of any ambiguity in the treaty, but also to the President’s application of the treaty to the facts in issue.”\textsuperscript{52} The court then added that this result also “is warranted given the President’s special competence in, and constitutional responsibility for, foreign affairs and the conduct of overseas military operations.”\textsuperscript{53} The court accordingly rejected Lindh’s bid for POW status and, by extension, his claim of combat immunity. Within a week of the decision, Lindh entered a guilty plea.\textsuperscript{54}

\textbf{C. The State Secrets Privilege}

Not all national security fact deference claims concern retrospective judgments as in \textit{Hamdi} and \textit{Lindh}. The executive branch also seeks deference on national security grounds in connection with \textit{predictions}. Such claims rely on familiar themes of comparative institutional competence, however, and they prompt familiar objections sounding in terms of the judiciary’s checking function. The debate regarding deference in the context of the state secrets privilege provides an apt illustration.

The question of deference in the context of the state secrets privilege arose in \textit{United States v. Reynolds}, a 1953 Supreme Court decision in which the government argued that “only the executive is in a position to estimate the full effects of . . . disclosure,” and that “unless the courts arc to interfere in the administration of Government, they must trust in the judgment of the appointed administrator.”\textsuperscript{55} The plaintiffs responded that such deference would be contrary to the separation of powers, since it would leave the

\textsuperscript{51} See id. at 556.
\textsuperscript{52} Id.
\textsuperscript{53} Id.
\textsuperscript{55} See Brief for the United States at 51–52, United States v. Reynolds, 345 U.S. 1 (1953) (No. 21).
executive branch unchecked. The Supreme Court, for its part, expressed sympathy for the separation of powers critique, warning that "[j]udicial control over the evidence in a case cannot be subordinated to the caprice of executive officers." It therefore framed the question in terms of the government's obligation "to satisfy the court" that disclosure might harm security. But the Court then went on to state that "where necessity is dubious" a mere "formal claim of privilege... will have to prevail," thus implying that judges should in fact give strong deference to the executive's claim in at least some contexts.

Perhaps not surprisingly, no one appears to know quite what to make of this guidance despite decades of subsequent litigation involving the state secrets privilege. A recent oral argument before the Ninth Circuit in Hepting v. AT&T, a civil suit alleging that the telecommunications industry assisted the National Security Agency in conducting illegal surveillance in the United States, illustrates the point:

Judge Harry Pregerson: Well, who decides whether... something's a state secret or not?

Deputy Solicitor General Gregory Garre: Ultimately, the courts do, Your Honor... And they... apply the utmost deference to the assertion of the privilege and the judgments of the people whose job it is to make predictive assessments of foreign—

Pregerson: Are you saying the courts are to rubberstamp the determination that the Executive makes that there's a state secret?

Garre: We are not, Your Honor, and we think that the courts play an important role—

---

56 Brief for the Respondents at 11, United States v. Reynolds, 345 U.S. 1 (1953) (No. 21).
57 United States v. Reynolds, 345 U.S. 1, 9-10 (1953). The Court stated that there was no need to address the "constitutional overtones" of these competing positions. Id. at 6. It necessarily spoke to them, however, when it resolved the merits.
58 Id. at 10. Where the plaintiff makes a strong showing of need for the information in question, moreover, the court cautioned that the executive's judgment "should not be lightly accepted." Id. at 11.
59 Id. at 11.
Pregerson: What is our job?

Garre: Your job is to determine whether or not the requirements of the privilege have been properly met. And that includes the declaration, the sworn declaration of the head of the agency asserting the privilege, and the assertion that that individual asserting it has personal knowledge of the matter [at hand].

Pregerson: So we just have to take the word of the members of the Executive Branch that tell us it's a state secret.

Garre: We don't—

Pregerson: [Because] that's what you're saying, isn't it?

Garre: No, Your Honor, what this Court's precedents say is the court has to give the utmost deference to the assertion, and the second part of the—

Pregerson: But what does "utmost deference" mean? We just bow to it?

Judge Michael D. Hawkins: It doesn't mean abdication, does it?

Garre: It does not mean abdication, Your Honor, but it means the court gives great deference to the judgments of the individuals whose job it is to assess whether or not the disclosure or non-disclosure of particular information would harm national security . . . .

The Ninth Circuit ultimately remanded in *Hepting* without reaching the merits, but the same panel did proceed to the merits in a closely related case. In *Al-Haramain Islamic Foundation v.*

---


44 See *Hepting v. AT&T Corp.*, 539 F.3d 1157, 1158 (9th Cir. 2008).
2009] National Security Fact Deference

Bush, the panel began by asserting the independent nature of judicial review:

We take very seriously our obligation to review the documents with a very careful, indeed a skeptical, eye, and not to accept at face value the government’s claim or justification of privilege. Simply saying “military secret,” “national security” or “terrorist threat” or invoking an ethereal fear that disclosure will threaten our nation is insufficient to support the privilege.\(^2\)

The court proceeded, however, to endorse a robust deference obligation: “we acknowledge the need to defer to the Executive on matters of foreign policy and national security and surely cannot legitimately find ourselves second guessing the Executive in this arena.”\(^3\)

This state of affairs has generated sharp criticism,\(^4\) and may yet result in legislative reforms.\(^5\) As things currently stand, however, deference in the state secrets scenario closely tracks the practice il-

---

\(^2\) Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1203 (9th Cir. 2007).

\(^3\) Id. See also El-Masri v. United States, 479 F.3d 296, 305, 312 (4th Cir. 2007) (asserting that “it is the court, not the Executive, that determines whether the state secrets privilege has been properly invoked,” but also that “the Executive and the intelligence agencies under his control occupy a position superior to that of the courts in evaluating the consequences of a release of sensitive information,” that the “executive branch’s expertise in predicting the potential consequences of intelligence disclosures is particularly important given the sophisticated nature of modern intelligence analysis,” and that “[i]n assessing the risk that such a disclosure might pose to national security, a court is obliged to accord the ‘utmost deference’ to the responsibilities of the executive branch”).

\(^4\) See, e.g., Examining the State Secrets Privilege: Protecting National Security While Preserving Accountability: Hearing on S. 2533 Before the S. Comm. on the Judiciary, 110th Cong. 2 (2008) (statement of Louis Fisher) (warning that deference—whether framed as “utmost deference” or just “deference” simpliciter—“undermines the principle of judicial independence, the essential safeguard of checks and balances, and the right of private litigants to have a fair hearing in court”) (transcript available at http://judiciary.senate.gov/testimony.cfm?id=3091&wit_id=6935); Reform of the State Secrets Privilege, Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 110th Cong. 56 (2008) (statement of William H. Webster) (arguing that “[i]f judges are well-qualified to review evidence purportedly subject to the privilege and make appropriate decisions as to whether disclosure of such information is likely to harm our national security”), available at http://judiciary.house.gov/hearings/printers/110th/40454.pdf.

illustrated in the other case studies. Courts are conscious that deference has costs in terms of reducing the judicial capacity to check the executive branch, but in some contexts they are loath to question the judgment of executive officials when push comes to shove.

D. Military Exigency and Preparedness

There are many other examples involving deference to predictive judgments in the national security context, including the national security exemption to the Freedom of Information Act (FOIA), the denial of security clearances, and the possibility that a detainee will be tortured if transferred to the custody of another state. But the paradigmatic examples of national security fact deference in the predictive setting involve claims of military necessity and preparedness.

The Supreme Court's 1827 decision in Martin v. Mott provides an early illustration of deference to a judgment of necessity. Jacob Mott refused to serve in the New York militia during the War of 1812 despite an order from President Madison calling forth the militia, and he was tried by court martial and fined for doing so. In subsequent litigation, Mott contended that Madison's order had been defective because the factual predicate for it—the existence

---

46 See FOIA, 5 U.S.C. § 552b(q)(1) (2006); Cent. Intelligence Agency v. Sims, 471 U.S. 159, 176, 179–80 (1985) (concluding that courts should defer to the judgment of the Director of Central Intelligence regarding whether to disclose the identity of intelligence sources in connection with a FOIA request, because courts "have little or no background in the delicate business of intelligence gathering," are less well positioned to make "complex political, historical, and psychological judgments" about the consequences of disclosure, and are not in the Director's position of being "familiar with the whole picture").

47 See Dept. of the Navy v. Egan, 484 U.S. 518, 529 (1988) (holding that "[p]redictive judgment" about the risks associated with granting a security clearance to an individual "must be made by those with the necessary expertise in protecting classified information," and that "it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment and to decide whether the agency should have been able to make the necessary affirmative prediction with confidence").

48 Cf. Munaf v. Geren, 128 S. Ct. 2207, 2212 (2008) (asserting that "[t]he judiciary is not suited to second-guess . . . determinations" by the State Department regarding the likelihood Iraqi authorities would abuse a prisoner).


of an imminent invasion threat—had not been satisfied. The Supreme Court declined to second guess Madison's judgment, however, on prudential and functional grounds. First, military discipline and effectiveness might be undermined if the President's determination were subject to question. Second, the President's determination might rest on intelligence that either would not be admissible in court or could not be disclosed publicly. Lack of judicial review increased the risk of abuse, Justice Story conceded, but in his view the remedy for that risk lay in a combination of electoral accountability and oversight from the legislature.

We find more recent—and cautionary—examples in the case law relating to the fate of Japanese Americans during World War II. In Hirabayashi v. United States the Supreme Court rejected a constitutional challenge to military orders imposing curfews on persons of Japanese ancestry on the West Coast. Among other things, the challenge raised the question whether the Court could review the predictive estimates underlying the orders, including the risk that the Japanese military might invade the West Coast, the likelihood that some persons of Japanese ancestry might prove disloyal, and the probability that such persons could be identified through an individualized screening process with enough precision and speed. The Court refused to closely scrutinize those judg-

---

72 See id. at 30–32. The New York Court of Appeals reached the same conclusion in Vanderheyden v. Young, 11 Johns. R. 150, 158–59 (N.Y. 1814).
73 See Martin, 25 U.S. at 30–31 (“The service is a military service, and the command of a military nature; and in such cases, every delay, and every obstacle, to an efficient and immediate compliance, necessarily tend to jeopardize the public interests.”).
74 Id. at 31.
75 See id. at 32. Justice Story also emphasized a presumption of virtuous character in high public officials. Id. at 32–33.
76 The Prize Cases provide another early example of deference to executive factual judgment where predictive and policy judgments intersect in a military setting. See 67 U.S. (2 Black) 635, 670 (1862) (holding that “[w]hether the President . . . has met with such armed hostile resistance . . . as will compel him to accord to them the character of belligerents, is a question to be decided by him, and this Court must be governed by the decisions and acts of the political department of the Government to which this power was entrusted”).
78 See id. at 89, 93–95; cf. Eric L. Muller, Hirabayashi: The Biggest Lie of the Greatest Generation 4–5 (Univ. of N.C. Legal Studies Research Paper 1233682), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1233682 (contending that the military did not in fact believe that there was a serious invasion threat, and that Jus-
ments. Later, in Korematsu v. United States, the Court confronted the same questions in connection with the subsequent military order requiring expulsion of Japanese Americans from the West Coast military district, and it reached the same conclusion. That the Court did not more closely scrutinize the factual predicates for these actions has occasioned extensive criticism, and understandably so. But the deeper flaw in these cases, arguably, was the Court’s failure to recognize that accepting these predicates did not require it to approve the constitutionality of these orders. The Court still could have identified a profound mismatch between the justifications offered by the government and the means selected to address them (that is, mass, long term exclusion on racial grounds without benefit of any individualized inquiry at any stage). Fact deference, even when warranted, does not require a judge to abandon independent judgment in the evaluation of the legal consequences of those facts.

The particular questions of exigency at issue in Mott, Hirabayashi, and Korematsu fortunately have not arisen again in more recent years. But the issue of deference with respect to military judgments continues to arise with some frequency in connection with less dramatic determinations relating to military preparedness. Courts reviewing the constitutionality of the military’s
“Don’t Ask, Don’t Tell” policy, for example, routinely state that they must defer to the judgment of military officers regarding the policy’s impact on military discipline and training in light of both functional and prudential concerns:

The Commander-in-Chief, the Secretary of Defense, the Secretary of the Army, and the generals have made the determination about homosexuality... and we, as judges, should not undertake to second-guess those with the direct responsibility for our armed forces. If a change of Army policy is to be made, we should leave it to those more familiar with military matters than are judges not selected on the basis of military knowledge. We... should not undertake to order such a risky change with possible consequence[s] we cannot safely evaluate.65

Similar themes pervaded the litigation in Winter v. Natural Resources Defense Council, Inc., which involved a challenge under the environmental laws to the Navy’s use of sonar in training exercises off the coast of California.66 At the district and circuit levels, judges determined that certain restraints could be placed on the use of the sonar without unduly disrupting the Navy’s capacity to train strike groups and certify them for deployment, despite the

Republican Case Against Judicial Deference to the Military, 5 Yale J.L. & Feminism 1, 5–6 (1992); John F. O’Connor, The Origins and Application of the Military Deference Doctrine, 35 Ga. L. Rev. 161, 280–83 (2000). Military deference, however, is both narrower and broader than national security fact deference. It is narrower in that national security fact deference extends beyond the military sphere, as illustrated by the discussion of the state secrets privilege. It is broader in that many “military deference” cases do not involve deference to factfinding but rather deference in the looser sense of constraining constitutional restraints more permissively in cases involving service members or military installations. See, e.g., Goldman v. Weinberger, 475 U.S. 503, 507 (1986) (“Our review of military regulations challenged on First Amendment grounds is far more deferential than constitutional review of similar laws or regulations designed for civilian society.”); Rostker v. Goldberg, 433 U.S. 519, 64–65 (1981) (“The case arises in the context of Congress’ authority over national defense and military affairs, and perhaps in no other area has the Court accorded Congress greater deference.”); Greer v. Spock, 424 U.S. 828, 837–38 (1976) (holding that crimes punishable by courts martial should not be held to the same vagueness standard as would apply to an ordinary criminal statute).

65 Ben Shalom v. Marsh, 881 F.2d 454, 461 (7th Cir. 1989); see also Thomason v. Perry, 80 F.3d 915, 923–26 (4th Cir. 1996) (citing comparative institutional competence and collateral consequence arguments in support of deference to military judgment regarding “Don’t Ask, Don’t Tell”).

contrary view of the Chief of Naval Operations (CNO). Ultimately, the Supreme Court sided with the government, emphasizing the "predictive" nature of the Navy officers' judgment en route to concluding that the lower court erred by not deferring to the CNO's judgment that the proposed restrictions would undermine naval preparedness. Justice Breyer foreshadowed that ruling in oral argument when he lamented:

I don't know anything about this. I'm not a naval officer. But if I see an admiral come along with an affidavit that says... that you've got to train people when there are [certain oceanic conditions], all right, or there will be subs hiding there with all kinds of terrible weapons, and he swears that under oath. And I see on the other side a district judge who just says, you're wrong, I then have to look to see what the basis is, because I know that district judge doesn't know about it, either.  

* * *

These case studies suggest considerable uncertainty regarding the justifications for national security fact deference. Whereas the Fourth Circuit and one Supreme Court Justice perceived a near-binding deference obligation in connection with enemy combatant status determinations, a plurality of Justices called for a non-deferential approach mediated by procedural innovations. The district judge in Lindh conceded that courts must retain authority to pass judgment on questions such as the Taliban's past compliance with the conditions of lawful belligerency, yet he gave the President's determination substantial if not binding weight nonetheless. The Ninth Circuit expressed concern for the independence of the judicial checking function in the state secrets context but ultimately proved unwilling to second guess the predictive estimates of Intelligence Community officials. Both the district court and the court of appeals in Winter were willing to disagree with the Navy's CNO

---


regarding the impact sonar restrictions might have on training, but the Supreme Court reversed.

This level of disagreement and uncertainty suggests that national security fact deference may be undertheorized; that is, courts and litigants may lack a shared foundation of understanding with respect to the legal nature of fact deference claims and the moves and arguments that accordingly are legitimate in resolving such claims. The rest of this paper aims to address this concern.

II. THE NATURE OF A FACT DEFERENCE CLAIM

What, precisely, is the nature of a fact deference claim, in the national security setting or otherwise? I contend in this Part that such claims are best understood through the lens of the “decision rules” literature in constitutional theory.\(^{90}\) The decision rules account nicely maps onto the existing practice of national security fact deference claims as described in the case studies above, helping us to understand why it is legitimate for litigants and judges alike to emphasize functional and prudential considerations.\(^{91}\) It also draws

---

\(^{90}\) The phrase derives from Mitchell N. Berman, Constitutional Decision Rules, 90 Va. L. Rev. 1, 9-13 (2004). For a sampling of additional contributions to this line of scholarship, see Richard H. Fallon, Jr., Implementing the Constitution 37-44 (2001) [hereinafter Fallon, Implementing]; Kermit Roosevelt III, The Myth of Judicial Activism: Making Sense of Supreme Court Decisions 11-64 (2006) [hereinafter Roosevelt, Myth]; Brannon P. Denning, The New Doctrinalism in Constitutional Scholarship and District of Columbia v. Heller, 75 Tenn. L. Rev. 789; Richard H. Fallon, Jr., Judically Manageable Standards and Constitutional Meaning, 119 Harv. L. Rev. 1275 (2006) [hereinafter Fallon, Judicially Manageable Standards]; Horwitz, supra note 3, at 1140-46; Kermit Roosevelt III, Constitutional Calcification: How the Law Becomes What the Court Does, 91 Va. L. Rev. 1649, 1658-66 (2005) [hereinafter Roosevelt, Calcification]; Catherine T. Struve, Constitutional Decision Rules for Juries, 37 Colum. Hum. Rts. L. Rev. 659 (2006). Other scholars have objected to the central claim in this literature that there exists a distinction between constitutional meaning and the rules that judges develop to permit implementation of that meaning in particular cases. See, e.g., Roderick M. Hills, Jr., Mistaking the Window-Dressing for the Window, 91 Judicature 146 (2007) (reviewing Roosevelt, Myth, supra). Though arguable, the criticism suggests that the distinction collapses because instrumental factors are central to the determination of constitutional meaning, and thus that implementation via “decision rules” is no more than further elaboration of meaning. If that is the case, this objection does not undermine the utility of relying on the decision rules literature as a guide to identifying the key instrumental considerations that might inform national security fact deference claims.

\(^{91}\) An alternative possibility is that fact deference claims are better understood as turning, in every instance, on the meaning and interrelationship among various consti-
Virginia Law Review [Vol. 95:1361

our attention to the nuances associated with those arguments, highlighting the possibility that they have been applied without sufficient rigor in actual practice. That insight in turn provides the foundation for a critical examination of the leading arguments for and against national security fact deference in the next Part.

A. Fact Deference as a Decision Rule (Constitutional or Otherwise)

Constitutional theorists in recent years have paid considerable attention to the "problematics of constitutional doctrine—what it is, how it compares to constitutional meaning, whether it is legitimate, how it should be employed, and what consequences follow." Professor Richard Fallon, for example, wrote in 2001 that:

tutional provisions such as the "judicial power" and "Commander-in-Chief" clauses. I find this account less compelling than the decision rules model, but it is worth noting because it might give rise to an originalist objection to reliance on functional and prudential considerations. Cf. Michael D. Ramsey, The Constitution's Text in Foreign Affairs 3 (2007) (contending that original public meaning can shed considerable light on seemingly sparse text relating to foreign affairs); Ingrid Wuerth, An Originalism for Foreign Affairs? 2–3 (Vand. Pub. Law Research Paper, Working Paper No. 08-13, 2008), available at http://ssrn.com/abstract=1134887 (urging foreign relations law scholars to take account of methodological debates in the constitutional theory literature). The important point for present purposes is that originalist methods likely would not produce an interpretation sufficient to resolve a fact deference claim, and that some degree of construction—potentially including resort to structural, functional, and prudential methods—thus would still be required. Cf. Randy E. Barnett, Restoring the Lost Constitution: The Presumption of Liberty 118–50 (2004) (discussing the propriety of such methods); Keith E. Whittington, Constitutional Construction: Divided Powers and Constitutional Meaning 5 (1999) (same); Lawrence B. Solum, District of Columbia v. Heller and Originalism 44 Nw. U. L. Rev. (forthcoming 2009), available at http://papers.ssrn.com/abstract=1241655 (elaborating the interpretation-construction distinction). If that is correct, the construction and decision rules accounts end up directing attention to similar concerns. Cf. Pearlstein, supra note 8, at 18 (noting that functionalism at times is unavoidable in resolving separation of powers disputes in the national security realm); Stephen I. Vladeck, Foreign Affairs Originalism in Youngstown's Shadow, 53 St. Louis U. L.J. 29, 31 (2008) (same). Of course, the text would have something to say if fact deference were invoked in the context of a factual question committed to a jury—which may explain why one does not see such attempts in actual practice. See U.S. Const. amends. V, VI, VII; cf. In re Winship, 397 U.S. 358, 364 (1970) (deriving a beyond-a-reasonable-doubt requirement from the Fifth Amendment Due Process Clause for the elements of a criminal charge).

Berman, supra note 50, at 5. Metadoctrinalism is not, of course, an entirely novel development. Several scholars credit articles in the 1970s by Henry Monaghan and Larry Sager with reviving interest in the distinction between constitutional meaning in the abstract and the judicially enforceable Constitution. See id. at 4–5 (discussing Henry P. Monaghan, The Supreme Court, 1974 Term—Foreword: Constitutional
judicially prescribed tests do not (and should not) always reflect the Court's direct assessment of constitutional meaning, but sometimes embody the Court's judgment about an appropriate standard of judicial review, indicating the circumstances in which other officials will be held by courts to have failed to meet their primary duties.\footnote{Fallon, Implementing, supra note 90, at 5–6 (emphasis omitted); see also Richard H. Fallon, Jr., The Supreme Court, 1996 Term—Foreword: Implementing the Constitution, 111 Harv. L. Rev. 54 (1997).}

This raised a question as to which considerations legitimately might inform such a judgment. Fallon rejected the notion that constitutional doctrine must seek to approximate constitutional meaning as perfectly as possible in order to be legitimate.\footnote{Id. at 10–11 (“This is especially true when the Court is unusually doubtful about the validity of what otherwise would be its own substantive judgment; when any injustice resulting from deference would not (in its judgment) be very great; and when there is a strong likelihood that independent judicial resolution would prove intensely unacceptable to large numbers of people whose views are not themselves unreasonable.”).} Nonetheless, he “appreciat[ed]” the urgency of assessing the grounds on which the Court determines whether to “employ its doctrine in a manner that would over- or underenforce constitutional meaning.”\footnote{Fallon, Implementing, supra note 90, at 7.} Ultimately, these and other considerations led Fallon to endorse a model in which “relatively robust judicial review” of the constitutionality of the actions of other government actors “is generally defensible, but the Supreme Court will sometimes have good reasons, rooted in concerns about the fair allocation of political power and its own comparative competence to reach sound decisions, to decline to displace the judgments of other institutions.”\footnote{Roosevelt, Calcification, supra note 90, at 1656 (discussing Sager’s article). James Bradley Thayer previously had drawn attention to a similar notion when he contended that courts should refrain from striking down a statute as unconstitutional in close cases. See, e.g., id. (citing James Bradley Thayer, The Origin and Scope of the American Doctrine of Constitutional Law, 7 Harv. L. Rev. 129, 139–44 (1893)). Roosevelt notes that Thayer did “not see himself as articulating anything new.” See id. at 1656 n.18 (citing, inter alia, Fletcher v. Peck, 10 U.S. (6 Cranch) 87, 128 (1810)).}
short, offered an institutionally contingent account of the formation of constitutional doctrine, one that emphasized comparative institutional competence and comparative institutional legitimacy.

Writing in a similar vein, Professor Mitch Berman elaborated that the general category of constitutional doctrine can be subdivided usefully into what he termed "constitutional operative propositions" and "constitutional decision rules." "Operative propositions, he explained, are doctrinal statements of constitutional meaning." In order for a judge to resolve a constitutional claim in a litigation setting, however, knowledge of the relevant operative proposition is not enough; operative propositions do not "self-implement" during litigation. A decisionmaker inevitably must determine, often in the face of disputed facts, whether the predicate elements of the operative proposition have been satisfied. In making that determination, the decisionmaker necessarily must employ some decisionmaking framework, including at least a burden of proof, even if only by default. Berman, supra note 90, at 51-60. Berman's primary purpose was to demonstrate the utility of maintaining the distinction between constitutional operative propositions and constitutional decision rules, despite criticism that constitutional adjudication is pragmatic "all the way up" rather than just at the decision rule stage or its equivalent. See id. at 60 (contending that "we can carve up constitutional doctrine into two sorts of rules...even while conceding the legitimacy of each, and without staking ourselves to any claims about the sorts of considerations upon which courts might rely in the derivation and formulation of either"); id. at 43-50 (summarizing the debate in terms of "whether it is meaningful to carve the universe of constitutional doctrine into conceptually distinct pieces" in light of the possibility that "constitutional adjudication is instrumental "all the way up"") (quoting Daryl J. Levinson, Rights Essentialism and Remedial Equilibration, 99 Colum. L. Rev. 857, 873 (1999)). Toward that end, Berman pointed out that deeper awareness of the distinction may enhance our understanding of the extent to which the Court's constitutional doctrine ought to bind other branches, and may also work against the undesirable tendency to assume that only judges have the capacity or responsibility for engaging in constitutional analysis. See id. at 84-87; cf. Paul A. Diller, When Congress Passes an Intentionally Unconstitutional Law: The Military Commissions Act of 2006, 61 SMU L. Rev. 281, 295-305 (2008) (criticizing legislators who supported legislation they believed to be unconstitutional).

9 Berman, supra note 90, at 9.

9 Id. at 10 ("A court cannot implement [an] operative proposition without some sort of procedure...for determining whether to adjudge the operative proposition satisfied," yet the court "lacks unmediated access to the true fact of the matter.") (emphasis omitted)); id. at 10 n.35 (noting that "epistemic uncertainty" on the judge's part requires selection of a burden of proof). In limited instances, the Constitution itself articulates the decision rule, in which case the distinction between decision rule
man labels these implementation rules "constitutional decision rules."  

Decision rules thus are not direct expressions of constitutional meaning. Rather, they are devices for operationalizing constitutional meaning in the context of a specific institutional setting. Some version of a decision rule ordinarily is unavoidable when judges (or, in some instances, juries\textsuperscript{102}) implement constitutional meaning, on this view. The point echoes Professor Richard Markovits' emphasis on the distinction between a test that embodies the requirements of constitutional meaning and the degree of proof a judge should require in determining whether elements of that test have been satisfied.\textsuperscript{102}

This account fits the national security fact deference scenario rather well.\textsuperscript{103} Indeed, the process of generating a decision rule routinely presents the question of whether a judge should give some weight—perhaps even binding weight—to another institution's decision, since other institutions routinely will have expressed their own view as to whether the predicate elements of an operative proposition are satisfied. That is to say, decision rules routinely manifest in terms of deference. Superintendant \textit{v. Hill}, a Supreme Court decision offered by Berman as an illustration of a constitu-

and operative proposition collapses. This is the case in connection with determinations of fact in criminal prosecutions, for example, where the Constitution mandates use of a beyond-a-reasonable-doubt standard. See Roosevelt, Ca\textit{cification}, supra note 90, at 1653. Constitutional silence with respect to the decision rule does not spare the judge the need to have one, however, but simply requires the judge to select the rule without the aid of clear textual direction. See id. at 1658.\textsuperscript{100}

\textsuperscript{100} See Berman, supra note 90, at 9-10; see also Roosevelt, Ca\textit{cification}, supra note 90, at 1652-54, 1657-58 (distinguishing between meaning and implementation rules).

\textsuperscript{101} See Struve, supra note 90 (pointing out that in some litigation contexts, compliance with constitutional operative propositions is determined by the jury rather than the judge, and noting that this may justify distinctive decision rules).

\textsuperscript{102} See Richard Markovits, Matters of Principle: Legitimate Legal Argument and Constitutional Interpretation 180-81, 215-16, 265 (1998). Markovits notes that these categories frequently are conflated by courts and commentators and points out that a test of meaning can be combined with a deferential standard of proof, or vice-versa. See id. at 180-81, 215-16. Solove makes a similar point when he contends that the impact of deference with respect to "factual and empirical evidence tends to override whatever level of scrutiny is applied, and is often dispositive." Solove, supra note 2, at 955.

\textsuperscript{103} Cf. Fallon, Implementing, supra note 90, at 116 (observing that "standards specifying . . . the deference due to other institutions of government cannot be derived directly from the written Constitution").
tional decision rule, demonstrates the point. In Hill, the Court had to determine what standard of review to employ in connection with a procedural due process challenge to a prison disciplinary board’s decision to revoke a prisoner’s good time credits. The Court determined that procedural due process is satisfied so long as the judge determines that a board had “some evidence” to support its conclusion. Rather than a statement regarding the meaning of due process, Berman argued, this deferential framework makes more sense when viewed as a decision rule reflecting the Court’s assessment that judges in most instances should defer to the judgments of prison disciplinary boards, intervening only in clear cases of mistake or malfeasance. Restating things a bit, Hill formulated a decision rule requiring judges to defer to the factual judgment of prison disciplinary boards except in extreme instances in which the existence of factual error is relatively clear.

To be sure, many fact deference scenarios do not concern implementation of constitutional operative propositions. The operative proposition at issue in Lindh, for example, derived from a treaty; the question was whether the Taliban had complied with the conditions of lawful belligerency specified in GPW Article 4. The operative proposition at issue in Hamdi—the proposition that the Authorization for Use of Military Force, as informed by the law of armed conflict, empowered the President to detain only certain personnel such as Taliban fighters—sounded primarily in statutory and international law. The state secrets privilege puts deference

106 See Berman, supra note 90, at 64–65.
108 Id. at 455–56. Berman notes that this rule may subsequently have been narrowed to apply only in connection with “insufficiency of the evidence” challenges, as distinct from claims based on alleged bias. See Berman, supra note 90, at 65 n.200 (citing Edwards v. Balisok, 520 U.S. 641, 648 (1997)).
109 Berman, supra note 90, at 64 (citing Fallon, Implementing, supra note 90, at 6, 38).
110 See supra text accompanying notes 32–35.
112 See supra text accompanying notes 21–26. The operative proposition at issue in Hamdi also can be viewed as a constitutional one if we take the view that it concerns the meaning of the Fifth Amendment’s due process requirement. Cf. Roosevelt, Myth, supra note 90, at 79 (contending that in Hamdi the “meaning of the Constitution [i.e., the operative proposition] is that the Executive may detain enemy combatants and not innocents”); Roosevelt, Calcification, supra note 90, at 1714–15 (same). Determining who counts as a detainable enemy combatant in that setting, however,
in issue in service of a common law evidentiary privilege, albeit one with strong claims to constitutional roots in at least some contexts. These deference scenarios involved decision rules, then, but not necessarily constitutional decision rules.\footnote{One might argue that all of these scenarios—indeed that any fact deference scenario—present a constitutional question with respect to the separation of powers. This may be so. The useful insight of the decision rules account, however, is that questions of deference should be examined in relation to the underlying operative proposition that gives rise to the need to resolve the deference question in the first instance, and those operative propositions in many instances will concern sources of law besides the Constitution.}

But it is difficult to see why this distinction should matter for present purposes. The abstract notion that there is a distinction between operative propositions embodying the meaning of legal rules and decision rules permitting judicial implementation of those propositions applies to any type of legal rule, be it constitutional, statutory, or of some other nature. A judge implementing a non-constitutional operative proposition is, after all, still subject to the same institutional restraints and the same epistemic uncertainty with respect to whether the predicate conditions of that proposition have been met. It thus would seem to follow that the insights of the constitutional decision rules literature—particularly insights relating to the process of decision rule formation—ought to apply by extension to other contexts.\footnote{Indeed, some such considerations might be more defensible in the context of sub-constitutional rules, given that it should be clearer in that context that Congress may override the Court's selection of a particular deference rule. Then again, one of the points of distinguishing operative propositions and decision rules in the constitutional theory literature is to draw attention to the possibility that Congress might have greater capacity to override the latter than the former even in the constitutional context. See Berman, supra note 90, at 25-27, 116-27 (emphasizing that decision rules do not share the Marbury-shielded nature of operative propositions).} I turn now to a survey of those insights, as a prelude to a close examination of how they might apply in the particular context of national security fact deference claims.
B. Decision Rule Formation and the Issue of Relevant Considerations

There is no comprehensive list of considerations that might legitimately inform the process of developing a decision rule, nor is there clear agreement regarding the criteria that might mark the boundaries of the relevant criteria set. Nonetheless, the recurrence of particular arguments in both the scholarly literature and the case law suggests a degree of consensus regarding the potential relevance of a number of considerations. For our purposes, we can develop these considerations into four distinct clusters: core accuracy, weighted accuracy, prudence, and legitimacy.

I. Core Accuracy

Perhaps the least controversial point about decision rule formation is that in determining how to implement an operative proposition a judge might consider the goal of core accuracy. That is to say, the judge might select a decision rule designed to maximize the chances of correctly determining whether the predicate conditions for satisfaction of an operative proposition have been met (even if we accept that doctrinal rules ultimately involve more than a quix-

---

13 See, e.g., Markovits, supra note 102, at 216–18 (identifying “factors that a judge is obligated to consider when deciding how much deference to show to a government decision-maker who has made the choice being challenged in a particular case,” including considerations of accuracy, comparative competence, impact on groups subjected to unconstitutional disadvantages as a historical matter, lack of deliberation, illicit motivations, and the status of the potential deferee); Berman, supra note 90, at 93 (providing a non-exhaustive list of “six analytically distinct factors or families of factors that might appeal to a judge considering whether, and how, to form a constitutional decision rule,” including “adjudicatory, deterrent, protective, fiscal, institutional, and substantive” considerations (emphasis omitted)); Roosevelt, Calcification, supra note 90, at 1638–66 (discussing “institutional competence,” “costs of error,” “frequency of unconstitutional action,” “legislative pathologies,” “enforcement costs,” and “guidance for other governmental actors”).

14 Core accuracy is an aspect of what Berman describes as the “adjudicatory consideration,” which he notes is “[t]he most obvious factor that a decision-rule-maker should consider.” Berman supra note 90, at 93. Roosevelt captures core accuracy concerns under the “Institutional Competence” heading. See Roosevelt, Calcification, supra note 90, at 1659–60. Markovits includes this concern, at least implicitly, under a consideration that could be labeled comparative institutional competence. See Markovits, supra note 102, at 216.
otic attempt at perfect implementation of abstract constitutional meaning). 15

The pursuit of core accuracy draws our attention to questions of comparative institutional competence. 16 If another institution is more likely than the court to resolve the relevant questions accurately, the court might be drawn to a decision rule incorporating deference to that institution’s decisions. 17 Professor Kermit Roosevelt illustrates the point when he notes that judges “may be poorly suited to gauge the necessities of administration in unusual environments such as prisons,” and that it “is generally conceded that judges are less able [than legislatures] to resolve complicated factual questions, such as the economic effects of a particular law.” 18

15 See Roosevelt, Calcification, supra note 90, at 1651–52.
16 See id. at 1659–60. Note that comparative competence for accuracy is not a one-size-fits-all proposition; the comparison may vary depending on the nature of the question. See Markovits, supra note 102, at 216 (observing that training, experience, and institutional structure render judges on the whole superior to other government actors at assessing values such as “fundamental fairness,” in contrast to the example of Defense Department superiority at collecting and examining “technical facts about national defense”); David Cole, No Reason to Believe: Radical Skepticism, Emergency Power, and Constitutional Constraint, 75 U. Chi. L. Rev. 1329, 1335–42 (2008) (reviewing Eric A. Posner & Adrian Vermeule, Terror in the Balance: Security, Liberty, and the Courts (2007)) (emphasizing the distinction between balancing competing government and individual interests and determining particular facts that might feed into that analysis).
17 See Roosevelt, Calcification, supra note 90, at 1659–61; cf. Christopher L. Eisgruber & Lawrence G. Sager, Civil Liberties in the Dragons’ Domain: Negotiating the Blurred Boundary between Domestic Law and Foreign Affairs after 9/11, in September 11 in History: A Watershed Moment? 163, 174–75 (Mary L. Dudziak ed., 2003) (presenting a comparative institutional competence argument regarding the contrasting epistemic capacities of military and civilian courts, in connection with the proposition that military life is a sphere apart from civilian life and hence that military courts are more likely “to get at the truth in disputes about the conduct of soldiers”).
18 Roosevelt, Calcification, supra note 90, at 1660 (citing, inter alia, Michael W. McConnell, Institutions and Interpretation: A Critique of City of Boerne v. Flores, 111 Harv. L. Rev. 153, 156 (1997)); cf. Fallon, Implementing, supra note 90, at 40–41 (noting that “in the face of uncertainty about whether it understands an institutional context, the Court may conclude that it would be imprudent not to defer to the judgments of others about what is appropriate under the circumstances,” and offering the example of deference to military and prison authorities). For empirical evidence suggesting that untrained judges perform poorly compared to trained judges when resolving complicated factual questions in the context of economics, see Michael R. Baye & Joshua D. Wright, Is Antitrust Too Complicated for Generalist Judges?: The Impact of Economic Complexity & Judicial Training on Appeals 23–24 (George Mason L. & Econ. Research Paper No. 09-07), available at http://ssrn.com/abstract=1319888.
In such circumstances, comparative institutional competence would appear to cut in favor of a deferential decision rule.

It is not enough to say, however, that judges should be alert to the possibility that another institution may have an edge in terms of accuracy. Capacity for accuracy is not a monolithic characteristic. The institutional comparison can and should be refined as much as possible in order to account for the distinct elements that combine to determine an institution’s capacity for accurate judgments. These elements include, at a minimum, each institution’s relative capacity to access relevant information, to access relevant expertise, and reliably to integrate these inputs in a manner that will minimize the risk of misfeasance or malfeasance in the decisionmaking process.

Each of these inquiries can and should be further refined, of course. Reliable integration, for example, constitutes a particularly important inquiry in this context in that it provides an opportunity for judicial review to function as a check against misfeasance or even malfeasance. Under this heading, therefore, one might expect judges to be mindful of red flags such as historical patterns of unreliability in particular contexts, the risk of democratic failure, and lack of deliberation (whether due to panic or otherwise).

---

19 See Solove, supra note 2, at 959 (noting the comparative expertise argument for deference claims).

20 For an exceptionally rich discussion of the nature of expertise and the dilemmas that arise when non-experts attempt to determine whether to credit the views of experts, see Scott Brewer, Scientific Expert Testimony and Intellectual Due Process, 107 Yale L.J. 1535 (1998) (unpacking the theoretical foundations of deference to expertise).

21 See Markovits, supra note 102, at 216 (arguing that “courts should defer less” where the decision in question “disadvantages a group, restricts a liberty, or deserves a value” where there is a historical pattern of such harms); id. at 217 (calling attention to structural, sociological, and historical evidence of a group’s capacity to protect itself in the ordinary political process, and noting that the presence of an illicit motive undermines the case for deference); Roosevelt, Calcification, supra note 90, at 1663–64 (referring to this as the “Frequency of Unconstitutional Action” consideration).

22 See Cole, supra note 116, at 1347–52; Roosevelt, Calcification, supra note 90, at 1664.

23 See Markovits, supra note 102, at 216–17.
2. Weighted Accuracy

Perfect enforcement is not the only accuracy-related consideration a judge may take into account in formulating a decision rule. Judges also may account for the possibility that the ultimate goal might not simply be to reduce the "sum total of adjudicatory errors"—the net false positives and false negatives—but might instead be to reduce the "sum total of weighted errors." That is to say, various factors might suggest that the decision rule should be calibrated to overenforce or underenforce the operative proposition rather than to pursue core accuracy. These factors might be specific to the litigants, or they might involve larger institutional concerns.

Consider first the possibility of weighting accuracy based on the interests of the litigants. We are familiar with the notion that in some contexts there may be more harm in a false positive than a false negative (a possibility memorialized in the cliché that it is better that ten guilty go free than one innocent go to jail), or vice-versa. The nature of the competing interests of the litigants in relation to the two types of error, on this view, will have much to say about the question of weighting. On one hand, an individual’s constitutional or other significant individual rights might be at stake. On the other hand, the government might be acting in pursuit of a particularly compelling interest, such as national defense. At the same time, the judge also should bear in mind societal interests that may not be clearly attributable to the litigants themselves but that nonetheless are directly implicated by the dispute in question, such as the Constitution’s commitment to separated powers and the rule of law.

Accuracy may also be weighted with reference to larger concerns associated with the creation of incentives that will have an impact on institutional behavior over time, though reliance on this

---

224 Berman, supra note 90, at 93 (emphasis added); see also Roosevelt, Calcification, supra note 90, at 1662 (labeling this the "costs of error" consideration).

225 The judge must account for such things as "the harm to the individual, the importance of the governmental interest likely to be thwarted, [and] the ability of the government to achieve its legitimate aims by other means." Roosevelt, Calcification, supra note 90, at 1662.
consideration may generate stronger legitimacy objections. A pattern of overenforcement of an operative proposition might have an inappropriate chilling effect on appropriate government behavior, for example, while a pattern of underenforcement might induce inappropriate government action. Bearing these risks in mind, courts might calibrate a decision rule to avoid them.

3. Prudence

Decision rule formation might also take account of factors having little or nothing to do with accuracy. Several such considera-

---

126 As we move away from core accuracy concerns, legitimacy objections to the consideration of particular factors arguably grow stronger. Cf. Berman, supra note 90, at 92 ("Just as only some sorts of moves are supposed permissible when traveling from the Constitution to constitutional meaning, ... maybe only some moves (albeit different ones) can fairly be relied on to support a given constitutional decision rule."). The legitimacy issue has been central to the metadiscourse discourse at least since Monaghan, who appreciated that doctrinal rules presented both separation of powers and federalism questions insofar as they were not derived directly from constitutional meaning yet purported to bind other branches of the federal government or the states. See id. at 88-89 (citing Monaghan, supra note 92, at 9, 22-23, 34-38). Indeed, Monaghan's solution—justifying judicially crafted constitutional doctrine as an exercise in specialized federal common lawmaking—prompted criticism along these very lines. See id. at 89-90 (citing Thomas S. Schrock & Robert C. Welsh, Reconsidering the Constitutional Common Law, 91 Harv. L. Rev. 1117, 1126-31 (1978)); cf. Sara Sun Beale, Reconsidering Supervisory Power in Criminal Cases: Constitutional and Statutory Limits on the Authority of the Federal Courts, 84 Colum. L. Rev. 1433, 1520-22 (1984) (concluding that specialized federal common law justified judicial development of doctrinal rules governing litigation procedure but not rules intended to govern extrinsic matters such as police investigative procedures). Some observers, however, presumably would not object to consideration of instrumental factors other than the pursuit of core accuracy. See Berman, supra note 90, at 14-15 (commenting on the argument that the task of ascertaining constitutional meaning is itself "shot through with judicial attention to practical, policy-oriented, and interest-balancing sorts of considerations," in the context of a discussion relating to David A. Strauss, The Ubiquity of Prophylactic Rules, 55 U. Chi. L. Rev. 190 (1988)).

127 See Berman, supra note 90, at 93-94 (discussing protective and deterrent considerations); Solove, supra note 2, at 1009 (noting risk that "hindsight" criticism may result in government paralysis in times of great urgency); cf. Roosevelt, Calcification, supra note 90, at 1666-67 (contending that "[u]ncertainty on the part of governmental actors may lead either to excessive timidity or to wasted resources when a good faith attempt to comply with constitutional demands is later held invalid").

128 See Berman, supra note 90, at 10 n.35 (observing that accuracy related considerations are "unavoidable," but "it does not follow that decision rules must be designed for the sole purpose of minimizing total [or weighted] adjudicatory errors that epistemic uncertainty produces").
tions can be gathered under the umbrella of prudential concerns, including efficiency, collateral impact, institutional self-preservation, and democratic accountability concerns.

Under the heading of efficiency, for example, a judge might formulate a decision rule in an effort to take advantage of another institution’s comparative advantage in factors such as speed (the amount of time required to resolve a dispute) or resource consumption (the monetary and other resources required to resolve a dispute).139 Some disputes may be particularly time or resource intensive, and some might even be beyond the reach of judicial proof under any realistic assessment of available private or public resources.140 In addition, decision rules might be crafted in hopes of optimizing such costs. Second, decision rules might be crafted to account for the collateral impact of litigation on other concerns such as related government operations or maintaining the secrecy of classified information.141

A third prudential consideration focuses on the possibility that adoption of a particular decision rule may tend either to shield the judiciary from or to expose it to institutional harms in the form of lost prestige, legitimacy, or political capital.142 Such blowback might flow directly from the “interbranch friction” generated by non-

---

139 See id. at 94–95 (discussing the “fiscal consideration” (emphasis omitted)).
140 Roosevelt accounts for similar concerns under the label “enforcement costs.” See Roosevelt, Calculation, supra note 90, at 1665 (“Some constitutional operative propositions may require courts to decide questions that they simply cannot, or that they cannot without burdensome or intrusive evidence-gathering.”); see also Solove, supra note 2, at 1007–08 (discussing the difficulty justification).
141 See Roosevelt, Calculation, supra note 90, at 1665 (discussing “enforcement costs” and related issues of “burdensome or intrusive evidence-gathering”). For a classic example of this argument in practice, see Johnson v. Eisentrager, 339 U.S. 763, 779 (1950) (emphasizing the intolerability during hostilities of causing military commanders to lose “prestige” or servicemen to leave their stations to participate in litigation).
142 Berman labels this the institutional consideration. See Berman, supra note 90, at 95. Berman notes that Alexander Bickel famously provided an institutional justification to support justiciability doctrines, though he also observes that Bickel’s account generated substantial criticism. See id. (citing Alexander M. Bickel, The Least Dangerous Branch: The Supreme Court at the Bar of Politics 184 (2d ed. 1986); Gerald Gunther, The Subtle Vices of the “Passive Virtue”—A Comment on Principle and Expediency in Judicial Review, 64 Colum. L. Rev. 1 (1964); Herbert Wechsler, Book Review, 75 Yale L.J. 672 (1966) (reviewing Alexander M. Bickel, The Least Dangerous Branch: The Supreme Court at the Bar of Politics (1962), and Alexander M. Bickel, Politics and the Warren Court (1965))).
deferential judicial review of the actions of other branches, or it might simply result from negative public reaction to perceptions of inappropriate judicial intervention in some particular area even in the absence of retaliation or threatened retaliation by another branch. On this view, awareness of the checking capacities of the other branches—and sensitivity to prevailing political opinion notwithstanding the judiciary’s theoretical insulation from politics—may contribute to decision rule formation.

Finally, a judge might formulate a decision rule in a manner that accounts for democratic accountability concerns. More specifically, a judge might conclude that ultimate responsibility for certain decisions—particularly those that shade into policy judgments—ought to rest with an institution that, unlike the judiciary, is subject to direct (or at least relatively direct) electoral accountability. As Professor Paul Horwitz observes in connection with the general phenomenon of judicial deference, the Supreme Court from time to time “has justified its deference to [the elected] branches on the grounds that they are more closely tied to the mechanisms of political accountability that legitimize and constrain the policy choices they make.” The democratic accountability concern collapses back into an institutional self-preservation argument insofar as a judge accounts for this factor simply as a proxy for the risk of political blowback. But giving weight to superior democratic accountability is not necessarily a question of institutional self-preservation. It is entirely possible for a judge to have regard for the value of democratic accountability even in the complete absence of retaliation fears.

4. Legitimacy

A final consideration involves comparative institutional legitimacy. Scholarship treating the general topic of deference fre-

---

13 Berman, supra note 90, at 95.
14 See Horwitz, supra note 3, at 1080–83.
15 Id. at 1082–83.
16 Berman identifies a further factor that may influence decision rule formation, labeling it the “substantive consideration.” See Berman, supra note 90, at 95 (emphasis omitted). This category refers to the possibility that “judges could conclude, based on their own substantive value or policy judgments, that a particular constitutional provision, properly interpreted, carries its underlying norm or principle too far or not far
2009] National Security Fact Deference 1399

quently emphasizes the significance of comparative legitimacy, sometimes citing it alongside comparative accuracy as the most pertinent factors in the analysis.137 It is not obvious, however, that this inquiry contributes something independent to the analysis in every instance.

In the context of a dispute between institutions regarding the allocation of decisionmaking authority, "legitimacy" could refer to a formal claim that some relevant source of law directly resolves the dispute. For example, one might argue that Article I, section 8 of the Constitution explicitly allocates to Congress the decision whether to declare war, and that Congress therefore is the legitimate decisionmaker when it comes to declaring war even if functional and prudential arguments would favor giving the President that decision. We might call that a "hard" legitimacy claim.

But "legitimacy" also might be used in conclusory fashion, as a mere label applied to the institution that prevails after an analysis that turns on factors other than formal claims of authority. To argue that one institution is a more legitimate decisionmaker than another in this sense is simply a shorthand way of saying that various functional or prudential factors warrant giving the authority to that institution.138 And, of course, some would say that all or at least most hard legitimacy claims on close inspection turn out to be of the soft variety.139

* * *

Not surprisingly, neither litigants nor judges in actual practice systematically canvass these decision rule criteria when national

---

137 See, e.g., Horwitz, supra note 3, at 1079-85 (citing, inter alia, Gary Lawson & Christopher D. Moore, The Executive Power of Interpretation, 81 Iowa L. Rev. 1267, 1278 (1996)).

138 Cf. Horwitz, supra note 3 at 1082-83 (categorizing democratic accountability concerns under the guise of comparative legitimacy).

139 Cf. Posting of Roderick M. Hills, Jr. to Prawfsblawg, Horowitz on Deference, Hills on Pragmatism, http://prawfsblawg.blogs.com/prawfsblawg/2008/03/horowitz-on-def.html (Mar. 10, 2008, 9:25 EST) (arguing, in response to Horwitz, supra note 3, that the distinction between comparative accuracy and comparative legitimacy collapses insofar as the criteria that define epistemic accuracy are the product of a normative choice that is in turn contingent upon the allocation of legal authority).
security fact deference disputes arise. This in itself is not necessarily problematic. Not all of these criteria would be pertinent in every instance, and in any event it would not be that remarkable for parties and courts to concentrate their attention on those criteria that seem most pertinent. The problem, instead, is the superficial treatment afforded those criteria that do receive consideration. Core accuracy concerns under the heading of comparative institutional competence arise frequently, for example, but rarely generate discussion beyond conclusory assertions of the executive's epistemic advantages vis-à-vis the courts. The same can be said for many if not all of the other considerations. This is not an appropriate state of affairs given the impact fact deference claims may have on the merits of litigation.

III. OBJECTIONS

Proposing to examine national security fact deference through the lens of the decision rules criteria might give rise to a number of objections, including objections to the very notion that legal concepts drive the decisions in this setting and objections to the role that the vague concept “national security” might play in resolving such disputes.

A. Window Dressing Objections

First, one might object that formal legal argument as a general proposition is mere window dressing, especially in connection with politically sensitive settings such as cases implicating national security. This objection comes in both weak and strong varieties.

The weak window dressing objection arises in relation to the pragmatist critique of the distinction between operative propositions and decision rules. Some scholars have objected to that distinction in the constitutional context on the ground that instrumental considerations—such as comparative epistemic competence and the prudential interest in preserving institutional prestige—are central to the task of determining constitutional meaning, and hence that there is no true distinction between operative propositions and

10 See supra Part I.
decision rules. By extension, one might argue that this Article's normative project to mine the decision rules literature in order to develop principles to guide resolution of national security fact deference claims is muddled. Even if the pragmatist critique is valid, however, it goes only to the surface and not the substance of my analysis. Insofar as instrumental considerations pervade legal analysis, this merely tends to confirm the need to engage in a nuanced way with core accuracy, weighted accuracy, prudence, and legitimacy concerns.

The strong window dressing critique, in contrast, is problematic. Or at least it is problematic if one brings the attitudinal model perspective to bear. That model "holds that the Supreme Court decides disputes in light of the facts of the case vis-à-vis the ideological attitudes and values of the justices." On this view, Supreme Court Justices are largely, if not entirely, at their liberty to pursue their policy or value preferences (consciously or not), while lower court judges may be equally free to do so at least in the absence of authority on point. It is a view that might have particularly strong explanatory force as the relevant legal materials grow more indeterminate and as the political salience of the underlying fact pattern increases. Both of these considerations may be characteristic of the national security fact deference scenario, suggesting there may be little point in deconstructing the factors involved in decision rule formation in that setting—aside perhaps from improving the quality of the window-dressing.

144 See, e.g., Hills, supra note 90, at 147; Hills, supra note 139.
147 Cf. Michael J. Klarman, From Jim Crow to Civil Rights: The Supreme Court and the Struggle for Racial Equality 4-5 (2006) (suggesting that discretion to indulge policy or value preferences relates inversely to the determinacy of the relevant legal materials).
The attitudinal model has its critics, of course, including those who defend the salience of legal concepts as a restraint on judicial decisionmaking. But the extent to which one side or the other has the better of the argument is well beyond the scope of this Article. I proceed on the assumption that for at least some judges the various factors associated with decision rule formation might indeed carry weight when the national security fact deference scenario arises.

B. DEFINITONAL OBJECTIONS TO "NATIONAL SECURITY"

A second set of potential objections accepts the relevance of legal analysis in relation to fact deference claims, but questions the role that might be played in that analysis by the concept "national security." This objection also takes two forms.

First, one might object to the use of "national security" to define a distinct subset of fact deference claims on the ground that there is nothing sufficiently distinctive about national security cases to warrant separate treatment. Litigation relating to public health or the national economy, for example, might involve equally high stakes or political sensitivity. But national security litigation might still be distinguished from these other scenarios in that the issues perceived as involving "national security" are more likely to generate questions regarding the legitimacy of judicial intervention.

Second, one might object that the meaning of "national security" in any event is too indeterminate to perform a distinguishing function. The phrase is vague in the sense that reasonable people will disagree regarding the range of matters that fall within its scope. Many observers have noted that the realm of "national security" extends beyond traditional concerns with military and espionage threats posed by other states, to include, for example, a variety of unconventional strategic concerns ranging from threats of violence

from non-state actors to issues such as pandemic preparedness, resource shortages, and economic crises.¹⁴⁶

Even if we were to narrow our focus to the traditional precincts of military and intelligence affairs, vagueness remains an issue. That definition no doubt would encompass combat operations, for example, but would it also extend to "military" matters such as a contract dispute relating to the purchase of military equipment or the regulation of "payday lending" on the outskirts of military facilities? Boundary disputes would still abound.

In light of these concerns, it would of course be unwise to let the label "national security" dictate outcomes when it comes to resolving fact deference claims. Fortunately, however, the mode of analysis developed in Part II avoids that error. The decision rule model calls for the judge to account for the nature of the government action or interest involved, to be sure, but it does so in a nuanced and particularized way. Categorizing a fact deference claim in terms of "national security" does not drive or predetermine the analysis, but instead simply frames and contextualizes the discussion, reminding us that the role of the judiciary is particularly contested in at least some such cases.¹⁴⁷

IV. TESTING THE JUSTIFICATIONS FOR NATIONAL SECURITY FACT DEFERENCE

The criteria for decision rule formation described in Part II cut against a one-size-fits-all model for resolution of national security


¹⁴⁷ Thus much, if not most, of the discussion below would apply by extension to fact deference claims having little or no relation to national security.
fact deference claims (or any other category of fact deference claim, for that matter). Many of these criteria are, after all, deeply dependent on case-specific elements such as the features of the decisionmaking process actually employed, the nature of the interests of the litigants, and the nature of the underlying operative proposition. Further parsing of these criteria as they might apply to a fact deference claim can, however, yield a number of useful insights. Together, these insights go some way toward shifting the analysis of such claims onto more coherent and defensible ground. By extension, these insights contribute to the larger project of assisting courts in defining an appropriate role in the national security setting.

A. Core Accuracy and Comparative Institutional Competence

Perhaps the single most important argument advanced in support of national security fact deference claims involves core accuracy. The government contends—and courts frequently agree—that the executive branch as an institution has a comparative advantage over the judiciary in terms of producing accurate judgments when it comes to at least some national security matters.\textsuperscript{16} Unfortunately, discussions of comparative accuracy all too often treat this inquiry superficially. Courts at times frame this question in a simplistic manner, with “the executive” and “the judiciary” treated in unrealistically monolithic terms,\textsuperscript{16} and “accuracy” itself examined without reference to its constituent elements.\textsuperscript{16} A more appropriate inquiry would account for a number of complicating considerations, including: the distinct elements that comprise epistemic competence, the distinction between retrospective and prospective factual judgment, and the complexities of decisionmaking procedures as they actually operate within the many distinct insti-

\textsuperscript{16} See also Fallon, Judicially Manageable Standards, supra note 90, at 1301.
\textsuperscript{16} Cf. Solove, supra note 2, at 1010–11 (criticizing monolithic depictions of institutions in connection with deference analyses, something he describes as characteristic of the legal process school).
\textsuperscript{16} For a related critique, see Pearlstein, supra note 8, at 14, 63 (criticizing willingness of commentators to assume the existence of the executive’s claimed functional advantages in terms of efficiency and accuracy).
tutions that collectively comprise "the executive." Disaggregating the comparative accuracy argument in this manner yields a more nuanced conclusion than conventional wisdom supplies.

1. Information Access

Consider first the question of access to information. All things being equal, an institution with superior ability to obtain relevant information should produce more accurate decisions than less well informed competitors. At first glance, this factor would seem to weigh heavily in favor of the executive branch. The executive branch contains a multitude of information gathering agencies. These include more than a dozen distinct agencies constituting the Intelligence Community, bringing vast technical and manpower resources to the task of information collection. They also include: the Office of the Director of National Intelligence, the various intelligence fusion centers, the Defense Department with its global network of geographic and functional commands, the State Department with its array of foreign service officers and embassies, the Justice Department with its growing network of overseas legal attachés, the Energy Department, the Commerce Department, and more than a few others as well. Indeed, it is no exaggeration to

---

115 Scholars including Christina Wells and Deborah Pearlstein have observed in commenting on comparative accuracy arguments in related contexts that this requires attention to be paid to the details of organizational structure and institutional incentives. See Christina E. Wells, Questioning Deference, 69 Mo. L. Rev. 503 (2004); Pearlstein, supra note 8.

116 See, e.g., Julian Ku & John Yoo, Hamdan v. Rumsfeld: The Functional Case for Foreign Affairs Deference to the Executive Branch, 23 Const. Comment. 179, 199-200 (2006) (observing that "courts have access to limited information in foreign affairs cases," in part because they "do not actively gather information" and in part because the information provided by parties "must survive rules that impose tests for relevance, credibility, and reliability that are designed to ensure fairness toward the contending parties").

117 The "Intelligence Community" is an interagency organizational concept that refers in practical terms to a host of agencies housed within a number of executive branch departments that are subject to a limited degree of centralized management and control in pursuit of the National Intelligence Program. For the list of components, see Members of the Intelligence Community: Who They Are, http://www.intelligence.gov/1-members.shtml (last visited May 18, 2009).

118 Of course, there is no guarantee that the information available to different departments and individuals in the executive branch will be pooled effectively (or at all). See Pearlstein, supra note 8, at 47-49, (discussing the stovepiping problem). Ques-
say that a considerable portion of the executive branch’s efforts are devoted to the acquisition of information. Much of this information relates to “national security” even if that phrase is defined narrowly in terms of military threats, much more so if that phrase is construed broadly.

The data collection process in federal court is, of course, quite different. Judges by and large do not directly engage in information collection and do not have the budget, personnel, or technology to do so on any significant scale even if they were so inclined. Instead, they depend on the litigants to collect and pass on information that may be relevant to resolving a factual dispute. This resource disparity suggests that the judiciary is at a distinct disadvantage. At least where the executive branch participates in the litigation, however, this distinction may be overstated.

Two factors complicate this institutional comparison. First, the relevant consideration is not an institution’s capacity to acquire information in the first instance, but rather its capacity to access information at the point when factfinding occurs. To the extent that the executive branch is willing to share with the court the information that it has collected, a judge ultimately might stand in the same position as would an executive branch decisionmaker in terms of the quantity and quality of data available to it.

To this one might object that the executive branch is unlikely to pass on the complete body of information available to it. Where information derives from classified sources or methods, the executive branch reasonably may fear that disclosure in litigation will cost it the ability to use that source or method in the future. Assume, for example, that a single decisionmaker faces this question. That person can be expected to consider this risk in comparison to the benefits that would follow from prevailing in the litigation, taking into account how withholding the information might impact the chances of prevailing. On at least some occasions, we can expect

---


18 See Ku & Yoo, supra note 152, at 199-205.
such a person to err on the side of protecting the information. Complicating matters, the choice may not be consolidated in the hands of a single decisionmaker, or at least not in the hands of a decisionmaker with a perceived stake in the success of the litigation. Indeed, it is possible that the decision will be in the hands not only of Justice Department officials (who have an institutional interest in pursuing litigation success) but also Intelligence Community officials (who have an institutional interest in preserving the confidentiality of intelligence sources and methods). Even within the Justice Department, in fact, there may be tension between the immediate interests associated with litigation success and the long-term interests associated with intelligence collection.\textsuperscript{156} Absent intervention at senior levels of the interagency process, therefore, initiative lies in the hands of the agency with control over the information in the first instance—which is to say that the information will not necessarily be released even when the litigation benefits of doing so might outweigh other costs.\textsuperscript{157} In a few instances, moreover, the decision may be affected by other use restrictions, as when a foreign intelligence agency provides information to the executive branch on condition that the information not be used in judicial proceedings or otherwise be made known to the public.

A second consideration further complicates the picture. Even if we assume that the executive branch as an initial matter has an informational advantage due to restraints on its ability to pass information through to the judge, this advantage could be offset thanks to information gathering advantages of the adversarial process. That process ensures the presence of a litigant other than the executive branch with substantial incentive to identify and present contrary information to the court. Even if we assume that the ex-


\textsuperscript{157} Cf. Jonathan M. Fredman, Intelligence Agencies, Law Enforcement, and the Prosecution Team, 16 Yale L. & Pol’y Rev. 331, 338 (1998) (discussing “discovery rights and the commensurate obligations that they place on prosecutors in cases that may involve Intelligence Community information”).
ecutive branch's own information collection resources are employed in a neutral manner such that available and relevant information will be collected regardless of whether it is consistent with a preferred outcome, we cannot also assume that its capacities are so broad as to acquire all information that an opposing litigant might be able to generate.

Since we cannot actually quantify and compare any of these gaps on a systemic basis, it becomes impossible to say with any certainty that the executive branch automatically has a comparative advantage over the judiciary with respect to access to information. Insofar as conventional wisdom assumes otherwise, it is too hasty. In some cases the executive will have such an advantage, in others it will not. The balance in a particular case depends on the extent to which executive branch decisionmakers have access to relevant information that they cannot or will not share with the court, and whether any resulting gap is offset by the court's access to additional information brought forward through the adversarial nature of the litigation process. Even when analyzed on a case-specific basis, it may prove impossible for a judge to determine with much confidence that one institution or the other has superior information access. Taken together, this cuts against placing much, if any, weight on this element in most instances.

2. Expertise

Accuracy does not turn solely on access to information, of course. Expertise matters as well. Here too conventional wisdom posits a substantial advantage for the executive branch. As with comparative information access, however, the comparative expertise inquiry turns out to be more complicated than conventional wisdom assumes.

As an initial matter, we must be clear regarding the precise identity of the decisionmakers subject to comparison on this dimension. Framing the question at a generic institutional level—"the executive branch" versus "the judiciary"—sheds little light, given that

---

198 For an insightful discussion of the progressive era roots of deference to expertise, and subsequent influences, see Solove, supra note 2, at 995–1003 (arguing that development of a deference principle facilitated application of constitutional restraints in the context of the emerging administrative state without thereby bogging down the courts in supervisory obligations).
factfinding is not literally carried out at that high a level of generality. Greater specification is needed, though it is not always supplied in actual practice.\textsuperscript{109}

In the judicial branch, factfinding decisions are made either by a judge or by a jury. Because deference arguably would present constitutional problems if employed in connection with questions committed to a jury (particularly in a criminal case),\textsuperscript{105} however, the question of national security fact deference arises primarily if not exclusively in the context of decisions made by a judge. As commentators and courts often observe, judges are generalists who typically have not studied, trained, or obtained practical experience in national security matters.\textsuperscript{161} Their epistemic competence, on this view, rests primarily on their generic intellectual assets, though it may be supplemented in some instances by expert witnesses put forward by the litigants or retained directly by the court.\textsuperscript{162} The executive branch, in contrast, contains a vast array of subject matter experts.\textsuperscript{163} Conventional wisdom holds that the executive branch prevails in this comparison, at least in the realm of national security affairs.

And that may well be correct. But does subject matter expertise always actually matter in resolving factual disputes? At times it will, and at times it will not. One cannot simply assume that it does and conclude on that basis that the executive has a comparative accuracy advantage.

Expertise often will matter a great deal when it comes to predictive factfinding in the national security setting, for example, just as

\textsuperscript{109} Such underspecification is a recurring problem in comparative institutional competence arguments. Cf. Adrian Vermeule, Many-Minds Arguments in Legal Theory, 1 J. Legal Analysis 1, 24–26, 35–38 (2009) (discussing the problem of underspecification in connection with arguments relating to majority rule, and noting that institutional comparisons frequently fail to account for the actual mechanisms of how decisions are made within institutions).

\textsuperscript{105} See supra note 91 (discussing constitutional restraints on deference in connection with questions committed to a jury).

\textsuperscript{161} See, e.g., Ku & Yoo, supra note 152, at 199–205.

\textsuperscript{162} For a sophisticated analysis of the theoretical obstacles non-experts face in assessing expert opinion in the trial setting, see Brewer, supra note 120; cf. Meredith Fuchs & G. Gregg Webb, Greasing the Wheels of Justice: Independent Experts in National Security Cases, 28 Nat’l Security L. Rep. 1 (Nov. 2006) (discussing the appointment of special masters to remedy a judge’s lack of expertise in national security affairs).

\textsuperscript{163} See, e.g., Ku & Yoo, supra note 152, at 200–05.
it does in other complex contexts. Specialized judgment lies at the heart of questions such as whether disclosure of a particular secret would be harmful to national security or whether a particular restraint on training would have an impact on military preparedness. Indeed, predictive judgments at times can be difficult to distinguish from policy judgments, in which case the comparative accuracy argument begins to intersect more overtly with the prudential concern for democratic accountability in the making of policy decisions and the closely related argument regarding "soft" legitimacy. Retrospective factfinding, in contrast, may be less likely in the ordinary case to require resort to special expertise. There are frequent exceptions, of course, as when a tort suit implicates complex questions of causation. But the paradigmatic questions of historical fact—who, what, where, when, and why—typically are within the ken of lay jurors and generalist judges.

Notably, judges from time to time emphasize the predictive nature

---

164 Julian Ku and John Yoo, for example, have argued that courts are especially bad at acquiring information relating to "broader political, economic, and social events and trends." Julian Ku & John Yoo, Beyond Formalism in Foreign Affairs: A Functional Approach to the Alien Tort Statute, 2004 Sup. Ct. Rev. 153, 195; see also Donald L. Horowitz, The Courts and Social Policy 274–84, 298 (1977) (describing ways in which institutional characteristics limit the reliability of judicial assessments of mutable "social facts," and commenting, in connection with the subject of judicial injunctions addressing complex social problems, that it may be "the inability of courts to see how their policies work out, or the difficulty of dealing with unusually fluid or broad problems in an episodic and narrow framework, that stamps the judicial process as more limited for some policy problems than other institutions are"); cf. Salove, supra note 2, at 962 (observing that "[c]ourts readily defer to legislatures when a statute involves forecasts and predictions").

165 Jack Goldsmith makes a similar point when he observes that judges are ill-suited to determine the content of U.S. foreign relations interests or the extent to which particular actions by states or other entities might run contrary to those interests. Jack L. Goldsmith, The New Formalism in United States Foreign Relations Law, 70 U. Colo. L. Rev. 1395, 1416–17 (1999). Goldsmith emphasizes that such inquiries "lack precise content" and that judges "lack the tools to make accurate and intelligent judgments in this context." Id. at 1417; cf. Curtis A. Bradley, Chevron Deference and Foreign Affairs, 86 Va. L. Rev. 649, 661–62 (2000) (observing that "courts often defer to the executive branch's assessment of United States foreign relations interests"). Much the same can be said about judicial review of any decisions that might best be described as turning on policy judgment.

166 Cf. Roosevelt, Calcification, supra note 90, at 1715 (observing that Hamdi's status was "a factual question courts seem quite capable of answering"); Roosevelt, Myth, supra note 90, at 231 (concluding that "[c]ourts are generally good at . . . deciding narrow factual questions").
of an executive judgment in the fact deference context, but one never sees an emphasis on the retrospective nature of such judgments.\textsuperscript{167}

None of this is to say that the comparative expertise inquiry can be resolved simply by identifying the factual dispute as forward- or backward-looking. Some predictions on close inspection will not depend upon expertise, and some retrospective judgments will. The historical/predictive distinction may be useful, but it cannot substitute for a contextualized inquiry into whether the nature of a particular dispute depends in some meaningful way on subject matter expertise. It does suggest, however, that judges should be especially sensitive to the possibility that some seemingly factual judgments have elements of policy discretion that trigger not just expertise concerns, but also accountability and legitimacy concerns as well.

3. Reliable Exploitation of Epistemic Resources

Having an institutional advantage in underlying epistemic resources, without more, does not ensure a superior factfinding process. Superior access to information or expertise contributes nothing to accuracy, after all, unless the decisionmaker actually exploits them, and does so reliably.\textsuperscript{168} This exploitation concern is a familiar insight in the context of the law of evidence and its treatment of expert witness testimony,\textsuperscript{169} yet it often goes unconsidered when comparative accuracy claims are made in the fact deference context.

\textsuperscript{167} See supra Part I.

\textsuperscript{168} See Markovits, supra note 102, at 217 (calling for less deference where a decisionmaker "did not actually investigate despite [its] capacity to do so" and noting that "circumstance and inclination as well as inherent skills affect the quality of decisionmaking").

\textsuperscript{169} See Fed. R. Evid. 702 ("If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.").
a. Non-Exploitation

Exploitation issues can arise in at least two ways. First, a decisionmaker may fail altogether to exploit an epistemic advantage. Consider, for example, how this might occur in a context in which the executive branch has an apparent advantage in terms of expertise. Indulging in generalization, we might say that factfinding decisions in the executive branch in theory can occur at the line level, the managerial level, the policymaking level, or even at the cabinet or presidential levels. Any one decisionmaker may have relevant expertise, but there is no guarantee at any of these levels that this will be so. Where the decisionmaker does not have personal expertise, of course, he or she can at least render a decision based on the recommendations or views of subordinates or other contributors who do have it. Again, however, one cannot simply assume that this has occurred. And we could say much the same thing with respect to whether the decisionmaker had access to relevant information. A comparative accuracy claim thus requires not just a showing of superior information or expertise, but also a case-specific showing that the decisionmaking process actually exploited such advantages.

b. Weighted or Unreliable Exploitation

Even if such a showing can be made, a second exploitation concern arises. Employing epistemic advantages means little, from a core accuracy perspective, if the decisionmaking process does not

---

90 In the context of the state secrets privilege, courts require formal consideration of the issue by the executive branch official heading the agency with responsibility for the information in question. See United States v. Reynolds, 345 U.S. 1, 7–8 (1953).

91 The prospect of multiple subject matter experts contributing to a factfinding judgment raises the question of whether any executive branch factfinding advantage should be deemed to be enhanced by virtue of the Condorcet Jury Theorem or other such “many-minds” arguments. See Vermeule, supra note 159. The better view is not. As Adrian Vermeule persuasively argues, commentators frequently err in assuming the presence of a “many-versus-one” scenario when conducting institutional competence comparisons. See id. at 33–38. The error lies in failing to recognize “epistemic bottlenecks.” Id. at 34–35 ("[T]he hierarchical structure of the executive usually implies that at some point a decision supported by many experts or mid-level officials will be funneled upward to a chokepoint, coming to rest on the desk of a single mind . . . . The fact that one or two minds must unavoidably make the decision, with limited epistemic competence, whether and when to accept the counsel of many minds is precisely what constitutes the epistemic bottleneck.")
actually aspire to core accuracy or if it suffers from defects that undermine its capacity to reach accurate judgments despite those advantages. Institutional incentive structures by happenstance or by design might tend to incentivize inaccurate factfinding, for example, while cognitive biases might undermine the reliability of individual and group decisionmaking even in the absence of such distorting motivations.\footnote{See, e.g., Cole, supra note 116, at 1342–58; Pearlstein, supra note 8, at 29–55; Geoffrey R. Stone, Civil Liberties v. National Security in the Law’s Open Areas, 86 B.U. L. Rev. 1315, 1328 (2006); Wells, supra note 151, at 921–35. But see Eric A. Posner & Adrian Vermeule, Terror in the Balance: Security, Liberty, and the Courts 64–75, 91–115 (2007); Ku & Yoo, supra note 152, at 199–205; Robert J. Puschaw, Jr., Defending Deference: A Response to Professors Epstein and Wells, 69 Mo. L. Rev. 959, 968–70 (2004); but cf. Adrian Vermeule, Judging under Uncertainty: An Institutional Theory of Legal Interpretation 77 (2006) (observing, in the context of interpretation, that the “general rubric of interpreters’ capacities can be broken down into motivational and cognitive components”)).

Consider first the possibility that an institution’s incentive structure might purposefully or incidentally motivate decisionmakers to err on the side of false positives or negatives. A hypothetical example illustrates the point. Assume that there is an executive branch official who must determine whether a particular individual ought to be placed on a terrorism watch list. Let us assume further that the decision is a close one on the merits, but all things being equal the official would determine on the merits that the person does not satisfy the relevant criteria. Will the official make that determination if he or she perceives substantial career risk in the event of a false positive, but little or no consequences in the event of a false negative? At least some officials in that scenario can be expected to err on the side of self-interest, consciously or not.\footnote{See, e.g., McNeal, supra note 156, at 22–23 (discussing incentives encouraging risk of false positives and discouraging risk of false negatives).} In that sense, incentive structures might produce judgments that differ from the dictates of expertise standing alone.\footnote{Judges, in contrast, enjoy a degree of institutionalized protection against this type of concern. Most notably, their jobs cannot be taken from them except upon impeachment, and their salaries may not be diminished. That protection is by no means complete—it is no salve to a judge’s conscience in the event of a catastrophic false negative, for example—but it is a notable institutional distinction nonetheless. Judicial decisionmaking also is distinct in that it is relatively transparent to the public (most rulings are public and accompanied by a reasoned explanation), and also in that it is subject to further review from other judges. These features produce direct and indirect forms of accountability, which in turn may constitute an additional institu-}
Indeed, we should not be surprised if organizations purposefully establish or knowingly tolerate such imbalanced incentive structures in circumstances in which the harms associated with a false negative are perceived to greatly outweigh the harms associated with a false positive—a scenario that might be especially likely to arise in settings related to national security.\textsuperscript{175} This is, of course, a type of weighted accuracy argument. And weighted accuracy arguments do have an important role to play in the resolution of fact deference claims, as I discuss in more detail in the next Section. But for present purposes the important point is that an argument for deference to the results produced by a weighted decisionmaking system must be defended on weighted accuracy grounds, not core accuracy.

A separate concern involves the unwitting influence of cognitive bias. Professor Christina Wells has emphasized this concern in her work critiquing the quality of decisionmaking by executive branch officials in the related context of emergency decisionmaking, and her concerns might well be extended to the national security fact deference scenario.\textsuperscript{176} Wells draws attention to the availability heuristic, which suggests that individuals are more likely to overestimate the chances an event will occur as that event becomes more "available" to them, measured with respect to how easy it is to call the event to mind.\textsuperscript{177} This risk is particularly acute in some national security settings, according to Wells, because the availability effect is stronger when the event in question is vivid or involves an "intense emotion such as fear."\textsuperscript{178} Wells notes that individual judgment...
also may be disrupted by such mechanisms as confirmation bias, overconfidence bias, and overestimation of risks that are "dreaded" (potentially fatal, involuntary, and over which there is no control) or "unknown" (new, unobservable, lacking immediacy, and not understood). Wells also observes that cognitive bias can distort the accuracy of group-based decisionmaking. Information cascades, for example, involve the risk that the presence of a person in a group holding a strong opinion "may influence others in the group who are less sure or who simply trust that individual's judgment." Reputational cascades, in turn, involve self-silencing of dissent in a group based on concern for one's reputation with other group members. Reputation cascades, Wells adds, can contribute to the pathology of "groupthink" in which "strivings for unanimity override...motivation to realistically appraise alternative courses of action." This risk is higher, moreover, when a group (i) is "insulated from outside influence," (ii) is homogenous, (iii) "lack[s] an impartial leader," (iv) "lack[s] systematic proce-

prospect for occurrence altogether in favor of "focusing on the possible harm from the outcome." Id. at 925; cf. Ron Suskind, The One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11, at 65 (2006) (describing the eponymous principle, allegedly embraced by Vice President Cheney, to the effect that certain threats were of a sufficient magnitude that "[i]f there was even a one percent chance of such an act occurring, we must act as if it's a certainty").

See id. at 923-24 (describing a tendency to overestimate the accuracy of one's own judgment, a tendency that grows more pronounced as the subject matter becomes less determinate and also in proportion to the expertise of the decisionmaker).

Id. at 924.


Wells, supra note 151, at 926.

Id.

Id. at 928 (quoting Irving L. Janis, Groupthink: Psychological Studies of Policy Decisions and Fiascoes 9 (2d ed. 1982)).
dures for evaluating evidence, and (v) "make[s] decisions in times of great stress." 186

These are serious concerns for any factfinding process, especially insofar as predictive judgments are concerned. 187 There are several reasons to be cautious before relying upon them to discredit executive claims of a comparative epistemic advantage over courts, however. First, some observers have cautioned that the results of cognitive bias studies might not generalize across institutional settings, and that it therefore may be unwise to premise legal reforms on those results. 188 Second, executive branch entities in at least some circumstances consciously structure decisionmaking in a manner that seeks to account for the flaws that might be introduced by such pathologies, as appears to be the case with at least some analytic activity within the Intelligence Community. 189 And third, we lack an account explaining why such flaws might have an impact on

186 Id. (citing Janis, supra note 185, at 176–77, 242–59); cf. Heidi Kitrosser, Classified Information Leaks and Free Speech, 2008 U. Ill. L. Rev. 881, 910 (contending that the "lack of an institutionally open, dialogic structure for executive branch decision making lends itself to a culture of 'groupthink' that secrecy fosters and exacerbates").

187 All of the mechanisms identified by Wells could impact predictive judgments, but only two of them (the Confirmation Trap and Overconfidence Bias) clearly would apply to retrospective determinations as well.


189 A review of materials made available to the public by the Central Intelligence Agency and the Defense Intelligence Agency reveals several studies informing analysts of these risks and advising how to minimize them, including Richards J. Heuer, Jr., Ctr. For the Study of Intelligence, Cent. Intelligence Agency, Psychology of Intelligence Analysis (1999), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PSYCHOINTELNEW.pdf; Jeffrey R. Cooper, Ctr. For the Study of Intelligence, Cent. Intelligence Agency, Curing Analytical Pathologies: Pathways to Improved Intelligence Analysis (2005), http://www.fas.org/irp/cia/product/curing.pdf. In a conversation with a knowledgeable official who asked not to be named, I was told that the Heuer text in particular is employed in training courses within the Intelligence Community.
executive branch judgments but not judicial judgments. Judges too are subject to cognitive pitfalls, after all, and thus the existence of a cognitive bias may not have an impact on the comparative accuracy inquiry.\footnote{See Wells, supra note 151, at 942; cf. Posner & Vermeule, supra note 172, at 75 (making a related argument about the mutual influence of "panic" on executive officials and judges). Note that group-based decision making can occur in both executive branch and judicial settings. Courts of appeals involve multiple members, for example, and there is reason to believe that their judgments can be influenced by group dynamics. See Sunstein, supra note 182, at 42 (discussing literature demonstrating polarization effects when judicial panels have ideological uniformity).}

In addition to these concerns, the question arises whether it is possible for a judge to operationalize concern for the distorting impact of cognitive bias.\footnote{Cf. Posner & Vermeule, supra note 172, at 74–86 (conceding the potential for misfeasance or malfeasance on an ad hoc basis, but denying that the case has been made for systemic predisposition to error or abuse).} Put simply, it is not clear how a judge would go about detecting the presence of cognitive bias in connection with a particular executive branch factual judgment. Both Christina Wells and Deborah Pearlstein have argued, however, that there may be a way to guard against the influence of cognitive bias on a systematic, untargeted basis.\footnote{Wells, supra note 151, at 936; Pearlstein, supra note 8, 55–65.} According to the literature exploring the effects of third party accountability on decisionmaking performance, decisionmakers who are aware that their judgments will be reviewed by an outsider under certain circumstances are more likely to:

(a) survey a wider range of conceivably relevant cues; (b) pay greater attention to the cues they use; (c) anticipate counter arguments, weigh their merits relatively impartially, and factor those that pass some threshold of plausibility into their overall opinion or assessment of the situation; and (d) gain greater awareness of their cognitive processes by regularly monitoring the cues that are allowed to influence judgment and choice.\footnote{Wells, supra note 151, at 938 (quoting Jennifer S. Lerner & Philip E. Tetlock, Accounting for the Effects of Accountability, 125 Psychol. Bull. 255, 263 (1999)).}

The accountability dynamic, in other words, incentivizes decisionmakers to self-police against the influence of cognitive biases and inappropriate institutional incentives of the type described above. To achieve this effect, research suggests that the decisionmakers
“must know in advance . . . that they will be accountable,” the “audience’s views on the topic must be unknown,” the “audience must be interested in process rather than outcome,” “the [reviewing] audience must be perceived as legitimately inquiring into the decision makers’ judgments,” and the audience must not be “easily tricked.” Where these conditions are met, Wells concludes, the resulting accountability dynamic “can improve the care that decisionmakers take and alleviate decisionmaking biases—even if the audience is less knowledgeable and subject to the same biases that plague the decisionmaker.”

The third party accountability dynamic arguably finds expression in the “hard look” review doctrine in the administrative law context, pursuant to which judges reviewing administrative agency rulemaking examine the reliability of the rulemaking process rather than its substantive result. Professor Matthew Stephenson has argued that “hard look” review makes judicial deference contingent on an agency’s willingness to engage in costly signaling in the form of constructing a sophisticated written record, and that this signaling account might extend to other deference scenarios involving claims of comparative institutional accuracy, such as judicial review of legislative factfinding—or, we might add, the national security fact deference scenario. Indeed, Wells argues for a “hard look” approach in the context of judicial review of executive decisionmaking in the emergency setting, and Professor Jonathan Masur argues explicitly for the direct incorporation of administrative law principles, including hard look review, when the executive seeks deference to its military judgment.

---

94 See id. at 940, 946 (emphasis added).
95 Id. at 942 (quoting Mark Seidenfeld, Cognitive Loafing, Social Conformity, and Judicial Review of Agency Rulemaking, 87 Cornell L. Rev. 486, 509 (2002)) (internal quotation marks omitted).
98 See id. at 793–800.
99 See Wells, supra note 151, at 945 (citing Seidenfeld, supra note 195, at 508–25).
100 See Masur, supra note 2, at 501–19.
What precisely would the court look for in conducting a process-oriented review? Judges can at least screen for evidence that the executive did make use of its purported epistemic advantages in reaching its judgment.\textsuperscript{301} A court could do this, for example, by requiring the executive branch to provide an express account of the decisionmaking process that produced the factual judgment. Courts already employ a variant of this procedure, in fact, in the context of the state secrets privilege. Courts may not accept a state secrets privilege claim without receiving a declaration from the official in charge of the responsible agency making clear that the official personally considered the question before concluding that disclosure of the information would pose an undue risk of harm to national security.\textsuperscript{302} Generalizing this approach, courts could require comparable declarations focused on the nature of the underlying decisionmaking process as a precondition to deference across the range of national security fact deference scenarios.

The benefits of such a screening process should not be overstated. Declarations no doubt would cast underlying decisionmaking processes in the best possible light, perhaps at substantial variance with events as they actually unfolded on the ground. Portions of them may have to be filed on an ex parte basis, moreover, as is done routinely in the context of the state secrets privilege. But they nonetheless would have some tendency to guard against deference claims that cannot truly be justified in terms of the executive's epistemic advantages.\textsuperscript{303}

\textsuperscript{301} This approach has an analogy in the context of judicial review of administrative agency factfinding. For the most part, judicial review of facts found by an administrative agency is deferential. Compare Administrative Procedure Act, 5 U.S.C. § 706(2)(A) (2006), with § 706(2)(E) (specifying, respectively, that a court may set aside agency actions that are arbitrary and capricious or actions that are not supported by "substantial evidence"). But APA, 5 U.S.C. § 706(2)(F) does open the door to non-deferential, de novo review where the agency's factfinding procedure was not itself reliable. See Citizens to Preserve Overton Park, Inc. v. Volpe, 401 U.S. 402, 415 (1971).

\textsuperscript{302} See United States v. Reynolds, 345 U.S. 1, 7–8 (1953).

\textsuperscript{303} Consider, in that regard, the fact that enemy combatant status determinations are made not by panels of experts having specialized knowledge of the jihad movement or other relevant expertise, but by panels of ordinary military officers. This may constitute a scenario in which the executive decisionmaker does not actually make use of information or expertise advantages that exist elsewhere in the executive branch.
B. Weighted Accuracy

The decision rules literature draws attention to the possibility that a judge may account for weighted accuracy considerations when determining how to respond to a national security fact deference claim. Such considerations may cut in either direction. That is to say, they may cut against deference in a scenario in which deference might otherwise seem appropriate on other grounds such as core accuracy. Or they may cut in favor of deference in a scenario in which other justifications for deference are lacking. Either way, however, weighted accuracy considerations are likely to prove difficult to assess in the national security setting.

Let us assume that a judge believes that the executive branch is less likely than the court to produce an accurate factual determination or at least that the executive is no more likely than the court to get the decision right in core accuracy terms. In the national security setting, we can expect the executive to argue that the court nonetheless should defer on weighted deference grounds. Specifically, the executive is likely to argue that it should receive extra latitude given the ostensible magnitude of its interest in preserving national security interests, and thus that the judge should adopt a decision rule, in the form of deference, that errs on the government's side. Consider, for example, the watch list scenario described above, in which the executive might claim that it is much more important to avoid a false negative than a false positive. That argument would carry no weight with a judge interested in pursuing core accuracy, as noted above, but it could prove dispositive for a judge open to a weighted accuracy argument in light of the government's claim that the stakes are especially high in that setting.

There are two potential problems with this line of reasoning. First, not all "national security" cases are alike, as noted earlier, and the interests potentially brought within the scope of that capacious phrase vary markedly in significance. Some interests may truly be paramount, others quite ordinary. Complicating matters, the comparative advantage the executive might have in terms of epistemic resources (discussed in the preceding section) may well come into play in the process of assessing the magnitude of a particular government interest, particularly insofar as such judgments have predictive or even policy judgment elements. A judge, in
short, may have difficulty determining just what to make of the executive's claim.

Second, and perhaps more significantly, there often will be weighted accuracy considerations cutting against a deferential posture. This is most obviously the case when the factual dispute pertains to the fundamental constitutional rights of a litigant, though it could be equally true for some rights claims of a different legal order, such as a physical liberty interest rooted in statute or treaty. More generally, the larger interest of society in ensuring that the government complies with the rule of law may also enter into the balance in the clash of competing weighted interest considerations.

In both respects, these tensions find an echo in the long running debate regarding the propriety of judicial deference to the factual judgments agencies make in the course of administrative adjudication. In 1932, the Supreme Court in *Crowell v. Benson*, held that while courts should defer entirely to agency resolutions of most adjudicatory facts (at least where the agency employed fair procedures), courts should not defer at all when reviewing disputed facts upon which the agency's jurisdiction specifically depended. *Crowell* also stated in dicta, moreover, that “[i]n cases brought to enforce constitutional rights, the judicial power of the United States necessarily extends to the independent determination of all questions, both of fact and law, necessary to the performance of that supreme function.” *Crowell*’s “jurisdictional fact” holding has been sharply criticized over the years, leading to questions as to its continuing vitality. Some contend, however, that at least the “constitutional fact” doctrine remains viable; indeed, Professor

---

284 Cf. Solove, supra note 2, at 946 n.19, 966-67 (observing that deference is “most problematic” in cases involving fundamental constitutional rights).
286 Id. at 60-61 (citing *Ng Fung Ho v. White*, 259 U.S. 276, 285 (1922) (holding that deportee claiming citizenship in habeas proceeding has right to independent judicial review of disputed facts)).
David Franklin concludes on this basis that fact deference is inappropriate in the enemy combatant scenario. In light of this discussion, a judge confronted with strong individual rights interests unopposed by strong governmental interests may well employ weighted deference as a justification for not deferring to the government even in circumstances where core accuracy concerns standing alone would have justified doing so. Whether the same is true when the government does have a strong competing interest, however, is much less clear. In that circumstance, it may be best to set weighted accuracy concerns aside altogether, lest the judge confront the unenviable—and potentially impossible—task of assigning relative weights to the interests in issue and then determining whether the resulting differential between those interests, if any, somehow justifies a particular modification to whatever level of deference might otherwise have been applied.

C. Prudence

The third cluster of potentially relevant factors involves prudential considerations independent of accuracy. Under this heading we find comparative institutional efficiency arguments, as well as concerns regarding the collateral impact a non-deferential decision rule might have on related government operations, the risk that the elected branches or the public will react to non-deferential review in a manner that could harm the judiciary as an institution, and related questions of democratic accountability. On close inspection, the efficiency and collateral impact inquiries prove to have little bite in the fact deference setting. The political blowback and democratic accountability concerns cannot be so easily dismissed.

---

26 See Franklin, supra note 2, at 1021–23; cf. Judah A. Schechter, Notes, De Novo Judicial Review of Administrative Agency Factual Determinations Implicating Constitutional Rights, 82 Colum. L. Rev. 1483, 1497–98 (1982) (reexamining traditional justifications for deferential review in the context of the CIA). This may be attributable to the apparent vitality of the constitutional fact doctrine in the context of appellate review of trial court factfinding in the First Amendment context. See, e.g., Boos Corp. v. Consumers Union of United States, Inc., 466 U.S. 485, 508 & n.27 (1984) (invoking constitutional fact doctrine to justify de novo review of factual disputes related to applicability of First Amendment protections). It may also reflect, however, continuing interest in the view that non-deferential factfinding remains an essential feature of the federal judicial power at least when constitutional rights are predicated upon such findings.
however, particularly in circumstances in which the "factual" dispute in issue shades into policy judgment.

1. Efficiency Concerns

The decision rules literature notes that judges may account for efficiency considerations in the course of decision rule formation, including the possibility that resolution of some issues will impose daunting fiscal or other resource requirements. The case studies draw attention to a distinct set of efficiency concerns by illustrating that the government and courts occasionally emphasize the executive's comparative advantage in terms of such efficiency features as speed. These efficiency concerns do have relevance in many settings. National security fact deference, however, is not one of them.

As an initial matter, the national security fact deference scenario does not automatically implicate concerns for the efficient allocation of fiscal or other resources—at least it is no more likely to do so in the abstract than any number of other litigation scenarios. The fact of the matter is that resolving factual disputes through litigation routinely involves a substantial commitment of resources by both the litigants and the public. Absent extraordinary circumstances, this factor standing alone does little to support the case for deference.

Other efficiency arguments are similarly unhelpful in this setting. When executive power is at issue, one frequently encounters com-

---

210 See supra text accompanying note 75–80. Writing about the role of comparative institutional competence arguments in connection with the allocation of government power during emergencies—a topic not unrelated to the issue of fact deference in national security cases—Philip Bobbitt offered the following observation:

Even if we agree ... that an attentiveness to the institutional capacities of the three branches would yield us a neutral principle of decision from which to derive rules for future disputes, how do we know that the Constitution is committed to making sure that the most efficient agency act in national emergencies? This seems plausible enough, but the design of the Constitution ... as well as its imposition of various cumbersome requirements on governmental action, suggests that a good many values are to be preferred to the calculus of administrative efficiency.

Philip Bobbitt, Constitutional Fate: Theory of the Constitution 55 (1982). Bobbitt aimed merely to show that one cannot easily escape inquiry into Constitutional purpose even when employing a non-purposive interpretive theory (because of the need to justify resort to that mode of argument), not to delegitimize consequentialism in general or efficiency arguments in particular.
parative efficiency arguments to the effect that decisions relating to national security must be made quickly or that it is important to have flexibility in taking up an issue as an initial matter or in revisiting a previous decision in light of changed information. Such claims have their roots in the Federalist No. 70, in which Alexander Hamilton famously defended the model of a singular president by pointing out that “[d]ecision, activity, secrecy, and dispatch will generally characterize the proceedings of one man in a much more eminent degree than the proceedings of any greater number.”211 These “Hamiltonian virtues,” as Pearlstein labels them,212 have long been cited as reasons to allocate authority to the executive branch in foreign and military affairs.213 But however relevant these virtues may be to such debates, we must resist the temptation to assume that they somehow shed light also on the national security fact deference scenario.

It is true, for example, that the executive branch can move far more quickly than can Congress or the courts.214 This is a relevant consideration insofar as the question at hand involves some need for alacrity, for example, whether the executive branch requires au-

211 The Federalist No. 70, at 392 (Alexander Hamilton) (Clinton Rossiter ed., 1961). The Hamiltonian Virtues play a key role in the Curtiss-Wright decision insofar as it awards inherent foreign affairs powers to the executive branch.


213 See Goldsmith, supra note 165, at 1397 (noting that “[c]onventional wisdom offers a functional justification for political branch hegemony in foreign relations”); Robert H. Knoles, American Hegemony and the Foreign Affairs Constitution 36 (N.Y. Univ. Pub. Law and Legal Theory Working Papers, Paper 111, 2009), available at http://ssrn.com/abstract=1111111 (context: nyu/piltwp (describing these features, along with comparative expertise, as “the pillars of special deference” to the executive in foreign affairs); Wells, supra note 151, at 906 (noting frequent reliance on the Hamiltonian virtues in support of deference claims); cf. Harold Hongju Koh, The National Security Constitution: Sharing Power after the Iran-Contra Affair 118–19 (1990) (observing that the structural features of the presidency renders that office “institutionally best suited to initiate government action,” and that the president’s “decision-making processes can take on degrees of speed, secrecy, flexibility, and efficiency that no other governmental institution can match”); Posner & Vermeule, supra note 172, at 16 (concluding that “both Congress and the judiciary defer to the executive during emergencies because of the executive’s institutional advantages in speed, secrecy, and decisiveness”).

214 See generally Posner & Vermeule, supra note 172, at 5, 18 (emphasizing the contrast along these dimensions); Ku & Yoo, supra note 164, at 188, 193–94 (same); Pushaw, supra note 172, at 968 (contrasting executive efficiency with a judiciary that “by design acts far more slowly than either political branch”).
2009] National Security Fact Deference 1425

Authorization from Congress before it can carry out some military function. But authority to act in exigent circumstances is not the question presented by national security fact deference. The executive’s ability to render judgments more quickly than the judiciary does not speak to the question whether a judge adjudicating a claim should defer to the executive’s previous factual judgment.

Much the same is true for the executive’s agenda-setting advantages. These advantages attach at both the front and back ends of the decisionmaking process, yet neither does much to advance the case for national security fact deference. On the front end, the executive’s advantage in terms of agenda control has to do with the possibility that courts simply will not have an occasion to reach an issue in the first instance because they must await a case or controversy presented by a litigant with standing.215 The executive, in contrast, can act at its own discretion and therefore address disputes as the need arises. This advantage has no relevance in the national security fact deference scenario, however, insofar as that scenario presupposes that the executive already has rendered its decision and that the particular issue has now come before a court in a posture suitable for adjudication.

The executive’s other agenda-setting advantage similarly fails to advance the case for fact deference. On the back end—that is, subsequent to an original decision—the executive branch as a general proposition has discretion to revisit decisions, whether in response to new information, new policies, or for no particular reason at all.216 The judiciary, in contrast, can revisit decisions only insofar as may be warranted by developments in actual cases, which in practical terms may mean relatively few such opportunities. The executive thus can engage in error correction more readily than can the

215 See, e.g., Ku & Yoo, supra note 164, at 182-83 (adding that litigation requires not just a willing and qualified litigant, but also one with sufficient resources to contest the case appropriately); Pushaw, supra note 172, at 968; cf. Posner & Vermeule, supra note 172, at 5 (describing the executive as flexible, the judiciary as rigid).

216 We see the executive employing this capacity, for example, in conducting annual reviews regarding the status of Guantanamo detainees who already have been classified, in the government’s eyes at least, as enemy combatants. For an overview of the “administrative review board” process, see Memorandum from Gordon R. England, Deputy Sec’y of Def., to Sec’y of Military Dep’ts (July 14, 2006), available at http://www.defenselink.mil/news/Aug2006/d20060809ARBPoliciesMemo.pdf (describing ARB procedures).
judiciary, which may experience a form of dead hand control simply as a result of the fact that no litigant has sought (or can seek) to reopen a question. But this advantage is inapposite to fact deference claims. Indeed, by emphasizing the virtues of a revisitation power in the abstract, the argument tends to reinforce the claim that original executive branch judgments may be flawed and in need of subsequent review. In any event, the fact that the executive itself can revisit the issue tells us nothing about whether the judiciary should be able to do so as well.

2. The Collateral Impact of Non-Deferential Review

Advocates of deference at times also emphasize the collateral consequences that non-deferential judicial review of executive branch factual judgments might have on related government operations or activities. On this view, the benefits of judicial review—measured in terms of enforcement of separation of powers values or even enhancement of accuracy—in some circumstances may be outweighed by collateral costs entailed by the very process of non-deferential, or insufficiently deferential, review.

When precisely does this argument come into play? Advocates of deference do not contend that collateral costs outweigh potential benefits in all national security related litigation. Indeed, the argument played no significant role in most of the examples surveyed in Part I. Most if not all judicial review of government action, after all, entails some degree of disruption to government operations. Government personnel, for example, often are obliged to spend some amount of time and resources participating, directly or indirectly, in the process of litigation, whether by serving as witnesses in a formal sense, gathering and reviewing documents, speaking informally with attorneys or investigators, and so forth. These litigation related activities to some extent are bound to disrupt the performance of ordinary government functions.

But some such disruptions are more serious than others. Disruption of military activity, for example, may impose unusually high costs. So said Justice Jackson in Johnson v. Eisentrager, a post-World War II decision denying habeas rights to a group of Ger-

---

217 See Ku & Yoo, supra note 164, at 183, 188-89, 192, 196-97.
mans convicted of war crimes and detained in a U.S. controlled fa-
cility in Germany. Jackson gave many reasons for the decision, but
placed particular emphasis on the undesirable practical con-
sequences that would, in his view, follow from permitting any judicial
review in this setting. These included: disruption of ongoing mili-
tary operations, expenditure of scarce military resources, distrac-
tion of field commanders, harm to the prestige of commanders, and
comfort to armed enemies. The government not surprisingly em-
phasized such concerns in the Hamdi litigation as well, though with
much less success; and similar arguments continue to play a signifi-
cant role today as courts grapple with still unresolved questions re-
garding the precise nature of habeas review of military determina-
tions of enemy combatant status.

But even in the enemy combatant setting, where disruption con-
cerns arguably are near their zenith, this argument does not neces-
sarily point in the direction of fact deference as the requisite solu-
tion. It did not persuade the Supreme Court in Hamdi to defer to
the government’s factual judgment, nor did it do so in the more re-
cent decision in Boumediene v. Bush dealing with noncitizen de-
tainees held at Guantánamo. The impact of the argument in those
cases instead was to prompt the Court to accept procedural innova-
tions designed to ameliorate the impact of judicial review, rather
than seeking to avoid that impact via deference. This is a useful
reminder that even when the executive branch raises a legitimate
concern in support of a fact deference argument, it does not follow
automatically that deference is the only mechanism by which the
judiciary can accommodate the concern.

This leaves the matter of secrecy. Secrecy relates to the collateral
consequences inquiry in the sense that failure to maintain se-
crecy with respect to national security information can have extra-
litigation consequences for government operations—as well as for

---

209 See id. at 778–79.
210 See supra text accompanying notes 7–11.
211 There may be circumstances in which collateral consequences of this sort might
not be capable of amelioration through procedural devices aside from deference. Ar-
guably Molt, involving President Madison’s determination of the need to call forth the
militia, provides such an example. Then again, a case such as Molt might more easily
be explained in terms of a combination of the comparative accuracy argument dis-
cussed above and the political blowback and democratic accountability concerns dis-
cussed below.
individuals or even society as a whole—ranging from the innocuous to the disastrous. Without a doubt this is a significant concern. But, again, it is not clear that deference is required in order to address it. Preservation of secrecy is precisely the reason that the state secrets privilege exists, of course, and it also is the motive for the Classified Information Procedures Act, which establishes a process through which judges work with the parties to develop unclassified substitutes for evidence that must be withheld on secrecy grounds.\(^{22}\)

3. **Institutional Self-Preservation**

Judicial involvement in national security litigation, as noted at the outset, poses unusual risks for the judiciary as an institution. Such cases are more likely than most to involve claims of special, or even exclusive, executive branch authority. They are more likely than most to involve a perception—on the part of the public, the government, or judges themselves—of unusually high stakes. They are more likely than most to be in the media spotlight and hence in view of the public in a meaningful sense. These cases are, as a result of all this, especially salient as a political matter. And therein lies the danger for the courts. Because of these elements, an inappropriate judicial intervention in national security litigation is unusually likely to generate a response from the other branches or the public at large that might harm the institutional interests of the judiciary, either by undermining its prestige and authority or perhaps even by triggering some form of concrete political response.

This concern traditionally finds expression through the political question doctrine, which in its prudential aspect functions to spare judges such risks. But just because a court determines that a case or an issue is justiciable does not mean that the institutional self-preservation concern has gone away or that a judge has lost sensitivity to it. National security fact deference provides a tempting opportunity for judges to accept the responsibility of adjudication.

while simultaneously reducing the degree of interbranch conflict and hence the risk of political blowback. We cannot expect judges to attribute deference decisions to this motivation, of course, but we must account for the possibility—even the likelihood—that such concerns will play some role.

4. *Democratic Accountability*

Federal judges are not subject to electoral accountability and are relatively insulated from other political constraints. The executive branch, in contrast, has a relatively strong democratic pedigree. The President is elected, may face reelection, and in some respects grows stronger or weaker in accordance with the polls. Other executive officials partake of this accountability to some extent, at least, by virtue of their own accountability, be it direct or indirect, to the President. On this view, executive branch decisions as a general proposition enjoy a stronger democratic pedigree than judicial rulings.

Ordinarily nothing follows from this. In some cases, however, the judge may believe that this disparity makes an important difference. In particular, the judge may conclude that some decisions ought to be left in the hands of a more politically accountable institution. It is an argument that arises from time to time in national security fact deference litigation.

One way to understand the role of such arguments is to view them simply as manifestations of the institutional self-preservation concern discussed above. That is, judges may cite the superior democratic accountability of the executive branch as a reason to believe that non-deferential review would generate an unacceptable risk of political blowback. But it is possible to conceive of a judge giving weight to comparative democratic accountability even in the absence of blowback concerns, reflecting a sincere belief that some questions are better left with more accountable institutions. That raises the question whether we can develop an account that may explain which kinds of factual disputes most plausibly implicate the democratic accountability concern.

It is helpful at this point to recall the distinction—emphasized above in connection with the discussion of comparative access to relevant expertise—among retrospective historical facts, predictions of future events, and matters that are best described as turn-
ing on opinion or policy judgment. It is difficult to see the democratic accountability argument for deference to determinations of historic facts. At the same time, it is easy to see the democratic accountability argument for deference to opinion and policy judgments. The hard cases involve predictive judgments of fact, which in at least some instances can be difficult to distinguish from opinion or policy judgment. Suffice to say, perhaps, that the line between factual determinations and opinion or policy judgment is a continuum, and that the democratic accountability argument begins weak but grows stronger as the opinion or policy elements wax.\footnote{322}

Judges contemplating the democratic accountability concern also must avoid indulging unrealistic assumptions about the degree to which an executive decision actually implicates democratic accountability. Consider, for example, the decisionmaking role of the Administrative Review Board (ARB) mechanism for Guantánamo detainees. The purpose of the ARB is not to determine the past conduct of a military detainee, but rather to predict what might happen should the detainee be released. As a predictive judgment, this scenario might be thought to implicate democratic accountability concerns. But the nature of the ARB's composition (with a panel of appointed military officers) and the non-transparent nature of its work (despite the intense public interest in the Guantánamo issue, few if any members of the public are aware of the ARB process in general, let alone of any particular decision an ARB might make) call into question whether there is a meaningful nexus between ARB decisions and democratic accountability. As a general proposition, executive branch decisionmakers will vary widely in terms of exposure to political incentives,\footnote{324} and the issues

\footnote{\text{The two justifications are not coextensive, however. The core accuracy argument, for example, requires a showing that epistemic advantages actually were employed, something that is not a relevant consideration for the democratic accountability inquiry.}}

\footnote{\text{See Fallon, Implementing, supra note 90, at 9 (observing that "most decisions that are subject to judicial review are not made by legislatures but by low-level officials and administrative agencies that lack any strong democratic mandate," where "the actual prospect of democratic intervention is often small"); Solove, supra note 2, at 1015 (noting lack of transparency and accountability in administrative decisionmaking).}}
they resolve will vary at least as widely in terms of their transparency and salience in the public's eye.\textsuperscript{255}

\section*{D. The Derivative Nature of Legitimacy}

A final consideration that may inform the deference issue is one that arises frequently in actual practice: comparative institutional legitimacy.\textsuperscript{256} On close inspection, however, this inquiry proves to have no content independent of the functional and prudential considerations discussed above.

When the executive branch argues for fact deference on legitimacy grounds, it is making a claim regarding the \textit{formal} allocation of decisionmaking authority as between it and the judiciary. That is to say, it is arguing that some dispositive source of law vests it with authority to resolve a factual dispute, regardless of whether this allocation makes sense from a functional or prudential perspective. And in theory, this could be the case. One can imagine constitutional text, for example, expressly allocating factfinding authority to the executive for some particular issue.\textsuperscript{257}

But the Constitution does not formally commit any particular factual questions to the executive, let alone a broader set of “national security” fact disputes. It certainly does not do so as a textual matter, and no such allocation can be derived through consideration of the “essential” qualities of the executive branch without revert to the functional and prudential arguments previously explored.\textsuperscript{258} Arguments from formal legitimacy in this sense generate more confusion than insight. In the final analysis, the concept of “legitimacy” is better understood as a label to be attached to the

\begin{itemize}
\item \textsuperscript{255} See Pearlstein, supra note 8, at 22 n.102.
\item \textsuperscript{256} Cf. Solove, supra note 2, at 1003–04 (observing, in the course of recounting affirmative arguments for deference, that “opinions involving deference depict judicial evaluation of factual judgments as an intrusion into the discretion of the officials and institutions under review”).
\item \textsuperscript{257} The Constitution arguably does commit some \textit{legal} and \textit{policy} decisions to the President, of course. Formal legitimacy thus might be a useful model for understanding why judges in some settings should not supplant executive branch \textit{policy} judgments.
\item \textsuperscript{258} I do not mean to suggest that the executive branch cannot make and act upon factual judgments. Obviously it does so constantly. The point instead is that the judiciary is not categorically excluded from reaching independent judgments when disputed facts relating to national security arise in a justiciable litigation setting.
\end{itemize}
institution that prevails in the functional and prudential analysis, not as an institutional quality that preexists such inquiries. 

***

Given the range, complexity, and indeterminacy of the considerations canvassed above, we can better appreciate why judges and litigants at times have struggled and spoken past one another in the national security fact deference context. The situation is not entirely hopeless, however. Careful parsing of these arguments does much to help us sketch the outline of a more coherent and defensible approach to resolving such claims. The key insights include:

- Comparative institutional accuracy arguments can favor the executive branch, but judges cannot assume that this is so simply because a factual dispute has national security connotations.
- Comparative accuracy can be a function of superior access to information or expertise, but in any event deference is not appropriate on this ground absent a showing that the decision actually exploited such advantages in a reliable manner.
- Judges should not be too quick to assume that executive agencies hold an advantage over the judiciary with respect to information access; the possibility that information can be passed through to the judge, combined with the potential for new information to emerge in the adversarial process, renders this inquiry unmanageable in many if not most instances.
- Special expertise is more likely to matter in the context of predictive judgments—which at times shade into opinion or policy judgment—than in the context of retrospective factfinding.
- Cognitive biases are significant concerns for any factfinding process, but it is unclear that judges are in a position to detect their presence. In any event, predicting deference on a showing that the executive reliably employed

---

29 Cf. Fallon, Judicially Manageable Standards, supra note 90, at 1291–92 (arguing that "judgments of nonjusticiability . . . tend to conjoin reasoning that emphasizes judicial incompetence with suggestions that the disputed questions are assigned to other branches").
epistemic advantages may guard indirectly against such concerns, via the third party accountability effect.

- Weighted accuracy concerns driven by the magnitude of the litigants' interests (the government's national security concerns, for example, or a private person's fundamental rights) are likely to be a wash in this setting, in which case it makes more sense to prioritize core accuracy and other prudential concerns.

- Efficiency concerns relating to speed, agenda control, and resource consumption ordinarily should have no impact on the fact deference question, however important they may be in other contexts.

- Prudential concerns regarding the collateral consequences of non-deferential review, including the risk of disrupting military operations or exposing classified information, are legitimate concerns, but they are better addressed through procedural devices such as the state secrets privilege.

- The fact that a national security related claim is justiciable does not mean that institutional self-preservation concerns drop out of the picture; fact deference provides a tempting—and not very transparent—opportunity for a judge to accommodate such prudential concerns.

- Democratic accountability concerns are weak with respect to retrospective factfinding, but they can be strong with respect to predictive judgments—particularly where the latter involves elements of opinion or policy judgment.

- Legitimacy concerns, understood as claims of formal allocation of authority to the executive branch, do no independent work in this context; on close inspection legitimacy arguments collapse into one or another of the functional and prudential concerns described above.

These insights are not a panacea for the problem of confusion in connection with national security fact deference claims (or fact deference claims more generally, for that matter). They leave much room for disagreement in particular cases. But they make a useful contribution nonetheless. Some frequently cited arguments simply are not relevant in this context; drawing attention to this helps to
dissuade future reliance upon them. Other arguments are potentially relevant, yet have a more limited reach than is often appreciated; drawing attention to this helps to produce more focused and relevant analyses. Together, these correctives can do much to decrease the cross-talk and uncertainty that currently plague fact deference claims.

CONCLUSION

The judicial role in national security affairs evolves constantly, reflecting the inevitable tension between the judiciary's reluctance to overstep its bounds in such a sensitive area and its obligation to adjudicate claims and thereby act as both guarantor of individual rights and as a check on the political branches. National security fact deference is a small but important thread in that larger tapestry, one that has become more significant in recent years. Unfortunately, it is not well understood, compounding the larger problem of uncertainty concerning the proper judicial role in this most significant of settings.

All of which would be of only mild interest, perhaps, if the pattern of arguments and outcomes in the actual resolution of national security fact deference claims gave reason to believe that litigants and judges shared at least a baseline understanding as to the nature of such claims and the sorts of considerations that might be relevant to resolving them. But that is not at all the pattern suggested by actual cases. One sees instead a hodgepodge of inchoate arguments with ample evidence of outright confusion and uncertainty. At the same time, a review of the role of fact deference claims in actual litigation suggests that such claims can have a dispositive impact. This is a poor state of affairs, to say the least.

The first step in shifting national security fact deference disputes onto a firmer foundation is to identify the nature of such claims. That inquiry is more complex than might appear at first glance. The most plausible account, however, depicts fact deference in general as a species of "decision rule," as that concept has been developed in the literature of constitutional theory. And that conclusion draws our attention to a series of arguments that scholars have identified as potentially relevant to the process of decision rule formation in general, including arguments that can be clustered
under the headings of (i) core accuracy, (ii) weighted accuracy, (iii) prudence, and (iv) legitimacy.

Examining these arguments as they may apply in the context of a national security fact deference claim does not yield a one-size-fits-all solution. Indeed, one of the core lessons of viewing such claims through the lens of the decision rules literature is that the deference question is deeply dependent on context, including the nature of the particular legal rule giving rise to the factual dispute, the nature of the interests of the litigants and of society that may be at stake in the case, and, especially, the precise nature of the "fact" in issue and the process by which the executive made a judgment concerning it. But parsing these factors nonetheless does yield insights that collectively can serve to shift the resolution of such claims onto much firmer ground. In brief, this approach calls for a de-emphasis on considerations such as formal legitimacy claims, comparative institutional efficiency, and collateral consequences for other government operations, and heightened (and more nuanced) attention to claims of comparative institutional accuracy and democratic accountability. This approach also highlights the unspoken role that institutional self-preservation concerns likely play in connection with many national security fact deference claims.

This article paints a complicated picture of the considerations that ought to inform resolution of national security fact deference claims, and purposefully so. One of the worst aspects of current practice is the tendency to oversimplify these arguments. At the same time, however, its insights simplify the analysis as a whole by clearing away a considerable amount of underbrush consisting of irrelevant or confused considerations. The net result is a more coherent and defensible approach to the deference question. And if the national security fact deference debate can be viewed as a microcosm of the larger tensions associated with the judicial role in national security affairs—and I think that it can—this would be a very welcome development indeed.
PANEL II:

INTELLIGENCE LAW DEVELOPMENTS

MODERATOR:
GEORGE JAMESON

The Development of Intelligence Law

W. George Jameson and Robert S. Litt

Over 30 years ago, in Washington, DC, the ABA’s Standing Committee on Law and National Security held its first workshop devoted to intelligence law. That timely look at intelligence and the law followed a period of national turmoil and inquiry, debate, and change in the conduct and oversight of intelligence. In his opening remarks, the Standing Committee’s Chairman, Morris Leibman, welcomed the participants and explained the motivation of the sponsors.

The explosion of problems in the intelligence field in the last two years moved us to begin an examination of this area of national security. Our preliminary research indicated that a whole new field of law was developing.

Although he recognized the need for future discussion of intelligence operations and practices, Mr. Leibman introduced the attendees to the workshop by noting the importance of law:

It is appropriate that we begin with the law for as the intelligence function has to be exercised in the real world, where life is often nasty, dangerous, solitary, brutish and short, so also does it have to be exercised by us in a manner consistent with the rule of law. The central challenge before our Committee is to assist in the formulation of rules for intelligence functions that at once protect the vital interests of the United States and the Constitution upon which it is founded.

Over the next two days, the workshop addressed three broad topic areas. It is notable how remarkably similar the concerns of 1979 were to those of 2012. The workshop organized its discussions to address:
ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

- The role of intelligence in national security law, including discussions about transnational terrorism, economic conflict, and the limits on national security intelligence in a free society.
- The continuing tensions between secrecy and disclosure, including legislative proposals to combat leaks and the role of the media.
- National security authorities, restrictions on the conduct of both foreign and domestic intelligence, and proposals to change those authorities and restrictions.

These issues, with some variations and sometimes different terminology, have long been and continue to be at the core of discussion about national security law generally and intelligence law in particular. Indeed, since the Revolutionary War and the adoption of the Constitution, actions of the Government relating to the protection of national security have stimulated discussion about the constitutional authorities of the three branches of Government, civil liberties concerns involving First and Fourth Amendment rights in particular, and a balancing of various national interests. The resulting dialogue has guided developments in the law to meet challenges facing the Nation—whether it be debates over the espionage laws and freedom of the press in 1917, the conduct of covert operations with or without congressional notification, or the appropriate means of gathering intelligence to counter terrorist threats.

The National Security Act of 1947

It has been said that the existence of a law on a matter reflects a need for it. And so the attack on Pearl Harbor led Congress, after the Second World War, to enact legislation designed to avoid another such surprise. The resulting National Security Act of 1947 included establishment of the National Security Council, the Department of Defense, and the Central Intelligence Agency, with a Director of Central Intelligence (DCI) as its head to enhance intelligence capabilities across the Government. The new national security system sought a more coordinated, but not a unitary, intelligence effort. The 1947 Act therefore placed responsibility for the correlation and evaluation of foreign intelligence of interest to the nation as a whole in the CIA, while leaving to the individual departments their responsibilities for intelligence of interest to their departments.

The law addressed the needs of the time. For example, it gave the CIA the authority to admit aliens into the U.S. from post-war Europe, to fire disloyal employees in the discretion of the DCI, to protect intelligence sources and methods, and to conduct other functions and duties related to intelligence as the President might direct. Significantly, an America wary of the police
powers that controlled Nazi Germany (and Soviet Russia) prohibited the
country's new foreign intelligence agency from having any internal security
or law enforcement functions. The Act was followed two years later with a
statutory grant of administrative authorities for the CIA to expend funds
for purposes necessary to carry out its functions "notwithstanding any other
provision of law."

For nearly 30 years, the CIA and other intelligence agencies—including
the National Security Agency and Defense Intelligence Agency, which were
established by Executive Branch directive and not by statute—operated under
this very general statutory authority and executive direction. It is only a slight
exaggeration to say that a search for the legal rules governing the conduct of
intelligence activities during the period 1947–1975 would find a general ab-
sence of such rules and, as noted by the Rockefeller Commission and Church
Committee in 1975, an absence of lawyers in the review of most operational
proposals and activities.

Reforms During the 1970s

But those inquiries—which followed significant revelations about the conduct
of intelligence activities within the United States, as well as activities directed
at Americans abroad—led to vigorous national debates about both intelligence
policy and intelligence law. This resulted in a significant increase in congressio-
nal oversight of intelligence activities (including establishment of the congress-
ional intelligence committees) and imposition of restrictions on the conduct
of those activities both in statute and in a series of executive orders, issued to
provide a structure and a set of rules for the Intelligence Community. These re-
strictions included a prohibition on assassinations and new processes to oversee
covert actions; new rules limiting collection of information on Americans limi-
ts and on intelligence activities in the U.S., including in particular a new law
(the Foreign Intelligence Surveillance Act) governing electronic surveillance
for intelligence purposes; limits on intelligence assistance to law enforcement;
requirements that Congress be notified of intelligence activity; and steps to
reorganize the existing intelligence structures.

The Standing Committee's 1979 workshop followed closely on this fer-
ment, and devoted attention to a variety of proposals to establish sweeping
"charter" legislation for the Intelligence Community, to more clearly distin-
guish domestic and foreign national security interests, and to consider the com-
plex problems of balancing privacy, openness, secrecy, and other interests while
taking care, in the words for President Ford, not to tie one hand behind our
back in fighting a national enemy.
ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

Continued Evolution Through the 1990s

The pendulum swung back towards a more aggressive approach to the conduct of intelligence activities in the 1980s, fueled in part by the more aggressive foreign policy of a new Administration. Whereas legislative efforts in the prior decade were generally intended to restrict intelligence activities, new laws attempted to assist authorized operational activity, even if only indirectly. Thus, Congress enacted the Classified Information Procedures Act (CIPA) to enable the Government to prosecute violations of the criminal law while still protecting intelligence sources, methods, and other classified information. The CIA also succeeded in exempting its operational files from the Freedom of Information Act, and Congress passed legislation to criminalize the disclosure of the identities of covert human agents. But this period of expansion of intelligence authorities culminated with the public exposure of and resulting trials over what has been called the Iran-Contra episode, leading to additional reporting requirements and controls on the conduct of covert action.

The period from the mid-1980s through 2001 brought dramatic changes in the environment in which intelligence activities were conducted. It began with the so-called “Year of the Spy” (1985)—an epitome of Cold War intelligence activities—but also saw the fall of the Berlin Wall and the breakup of the Soviet Union. Some called for, and Congress enacted, more organizational changes to enable the DCI to improve efficiency, collaboration, and information sharing across the intelligence and other national security communities—defense and law enforcement—to address the increasing problems of transnational crime. There was an increased awareness that terrorism, narcotics, and weapons of mass destruction had implications for the national intelligence, law enforcement, and defense communities and that collaboration among those communities—in part through improved collection and sharing of intelligence rather than continued sowing pipings of efforts—was essential to national security interests. At the same time, the end of the Cold War led to a decline in the overall emphasis on, and resources devoted to, intelligence.

September 11-Related Reforms

All that changed on September 11, 2001, perhaps the most defining moment in the history of U.S. intelligence since the attack on Pearl Harbor. In the years following the calamities in New York and at the Pentagon two major commissions investigated perceived failures of the Intelligence
Community (relating to the terrorist attacks on 9/11 and the misreading of Iraq’s weapons of mass destruction capabilities), leading to passage of laws to increase information sharing and collaboration both within and among intelligence agencies and with agencies outside the intelligence community. These laws included most notably the Intelligence Reform and Terrorism Prevention Act (IRTPA), which created the position of Director of National Intelligence to assume the coordination function previously vested in the DCI. In addition, the FBI transformed itself and now has a primary foreign intelligence mission, and cooperation and exchange of information among intelligence, military and law enforcement agencies in counterterrorism has increased. Congress also provided increased authority to collect intelligence and counterterrorism information, in controversial laws such as the USA PATRIOT Act and the FISA Amendments Act. But in addition, the rise of counterterrorism as the center of national security policy, and the new authorities granted the intelligence community, led—once again—to vigorous public debates about the intelligence law, including to detain, interrogate and try terrorists, and the proper role of intelligence agencies in counterterrorism.

Ongoing Challenges

Intelligence law therefore continues to pose challenging questions for lawyers. To a great extent, these mirror the themes addressed in the Standing Committee’s 1979 conference: Constitutional authorities and separation of powers; civil liberties—First and Fourth Amendments; balancing various national security interests; and the overarching principle of the rule of law. As the 21st century enters its second decade—and the Standing Committee its second half century—these big themes will play out across questions such as: what is the proper role of intelligence in defending the nation against cyber attacks? In an era where intelligence, law enforcement and military activity seem to converge, where should the lines between those activities—if any—be drawn? In the era of Facebook™, Twitter™ and the Internet, what restrictions should be imposed on collection and dissemination of information about not only Americans but foreign terrorists? How should intelligence operations be conducted in light of the civil liberties concerns and the advance of technology? What are the implications of international law on the conduct of U.S. operations in a world that is undeniably more “flat” than it was in 1947? And how do you maximize the sharing of information across networks, while protecting sensitive information from improper disclosure?
ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

Recommended Materials

The reference materials presented in this chapter attempt to provide a survey of these issues. They include two articles by General Counsels of the Central Intelligence Agency, written over thirty years apart, outlining the role of law and lawyers in the intelligence community; relevant portions of some of the foundational legal documents governing the activities of the intelligence community; and excerpts from some of the conclusions and recommendations of the key inquiries that have shaped intelligence law today. The electronic version of this document includes links to further resources.
ABA 50th Compilation References

3 July 2012

Background and History (General)

Available at: http://history-matters.com/archive/contents/church/contents_church_reports_rockcomm.htm

U.S. Congress, Senate Select Committee to Study Governmental Activities with Respect to Intelligence Activities [Church Committee] (1976).
Available at: http://www.intelligence.senate.gov/pdfs94th/s4intelligence_activities_V.pdf


Available at: http://www.9-11commission.gov/report/index.htm

Available at: https://www.cia.gov/library-center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article01.html

Available at: http://www.gpo.gov/fdsys/pkg/GPO-IC21/content-detail.html
ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY


Available at: http://www.gwu.edu/-nsarchiv/NSAEBB/NSAEBB144/document%204.pdf


Legal and Policy Framework

COMPILATIONS

Intelligence Community Legal Reference Book, Office of General Counsel, Office of the Director of National Intelligence


STATUTES

National Security Act of 1947, as amended
Available at: http://intelligence.senate.gov/nssact1947.pdf

Central Intelligence Agency Act of 1949, as amended
Available at: http://www.law.cornell.edu/uscode/text/50/403-1

National Security Agency Act of 1959
Available at: http://www.intelligence.senate.gov/nssact1959.htm

Available at: http://cryptome.org/jza/50usc421.htm

Foreign Intelligence Surveillance Act of 1978, as amended
Available at: http://www.law.cornell.edu/uscode/text/50/chapter-36

68

158
50th Anniversary

National Imagery and Mapping Agency Act of 1996
Available at: http://www.fas.org/irp/doddir/dod/d5105_60.htm

Homeland Security Act of 2002
Available at: http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

Intelligence Reform and Terrorism Prevention Act of 2004 [IRTPA]
Available at: http://www.nctc.gov/docs/pl108_458.pdf

Department of Defense, Title 10 Authorities
Available at: http://www.fas.org/irp/offdocs/laws/uscode10.html

Counterintelligence and Security Enhancements Act of 1994
Available at: http://www.govtrack.us/congress/bills/103/s2056

Counterintelligence Enhancement Act of 2002
Available at: http://www.law.cornell.edu/uscode/text/50/402b

Directives

Available at: http://www.fas.org/irp/offdocs/eo/eo-13470.htm

Available at: http://www.fas.org/irp/dni/icd/icd-1.pdf

Intelligence Community Directive Number 101, Intelligence Community Policy System (2009).
Available at: http://www.dni.gov/electronic_reading_room/ICD_101.pdf

Executive Order 11905 (Gerald Ford).
Available at: http://www.fas.org/irp/offdocs/eo/eo-11985.htm

Executive Order 12036 (Jimmy Carter).
Available at: http://www.fas.org/irp/offdocs/eo/eo-12036.htm

Other

References—Selected Topics

Covert Action

National Security Act of 1947, as amended
Available at: http://intelligence.senate.gov/nsaact1947.pdf

Central Intelligence Agency Act of 1949, as amended
Available at: http://www.law.cornell.edu/uscode/text/50/403-1

United States Code, Title 18 (sections 956-960, "neutrality" laws)
Available at: http://codes.lp.findlaw.com/uscode/18/I/45/960/

Executive Order 13440, "Interpretation of the Geneva Conventions Common Article 3 as Applied to a Program of Detention and Interrogation Operated by the Central Intelligence Agency" (2007).
Available at: http://www.fas.org/irp/offdocs/eo/eo-13440.htm

Available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d098:HR.2968

Available at: http://www.law.cornell.edu/uscode/text/50/chapter-33

(codified as amended at 22 U.S.C. § 2422 (1976)) repealed by Intelligence Authorization Act,


Oversight

SOTH ANNIVERSARY

Available at: http://www.fas.org/irp/cia/product/snider.pdf
S. Res. 400 (1976) (Senate Select Committee on Intelligence)

H. Res. 658 (1977) (House Permanent Select Committee on Intelligence)

National Security Act of 1947, as amended (Sections 501 et. seq.)
Available at: http://intelligence.senate.gov/nsact1947.pdf

CIA Act of 1949, as amended (Inspector General)
Available at: http://www.law.cornell.edu/uscode/text/50/403a

Executive Order 13462, President’s Intelligence Advisory Board and Intelligence Oversight Board (2008).
Available at: http://www.fas.org/irp/offdocs/eo/eo-13462.htm

Criteria on Thresholds for Reporting Intelligence Oversight Matters and Instructions Relating to Formatting and Scheduling, Office of the DNI (2008).

Information Sharing and Protection

United States Code, Title 18 (sections 793, 794, 798)
Available at:
http://www.law.cornell.edu/uscode/text/18/793 (793)
http://www.law.cornell.edu/uscode/text/18/794 (794)
http://www.law.cornell.edu/uscode/text/18/798 (798)

Communications Act of 1934 (unauthorized publication)
Available at: http://www.law.cornell.edu/uscode/text/18/798

Securities Exchange Act of 1934, as amended (exemption for intelligence)
Available at: http://www.sec.gov/about/laws/sea34.pdf

Internal Security Act of 1950
Available at: http://wadsworth.com/history_d/special_features/lrln_legacy/wxwc2c01c/content/wciv2/readings/mccarr1.html

National Security Agency Act of 1959 (Title III)
Available at: http://intelligence.senate.gov/nsaact1959.htm

Freedom of Information Act, as amended [exemptions (b) (1) & (3)] (1974).
Available at: http://www.justice.gov/oip/amended-foia-redlined-2010.pdf

71
ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

Privacy Act (1974)
Available at: http://www.justice.gov/opcl/privstat.htm

Right to Financial Privacy Act of 1978 (exemption for intelligence)
Available at: http://www.accessreports.com/statutes/RFPA.htm

Classified Information Procedures Act (1980).
Available at: http://www.law.cornell.edu/uscode/html/uscode18a/usccap_05_18_10_sq3.html

Intelligence Identities Protection Act of 1982
Available at: http://www.fas.org/irp/offdocs/laws/iipa.html


Executive Order 13526, Classified National Security Information (2009) [See also Executive Orders 13292, 12958, 12356, 11652]

Available at:

Executive Order 12968, Access to Classified Information (1995). Available at:

Available at: http://www.fas.org/sgp/bush/cui.html

Intelligence Community Directive Number 501, Discovery and Dissemination or Retrieval of Information within the Intelligence Community (2009).
Available at: http://www.dni.gov/electronic_reading_room/ICD_501.pdf

Intelligence and Law Enforcement

National Security Act of 1947 (law enforcement proviso)
Available at: http://www.intelligence.senate.gov/nssacl1959.htm

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 [USA PATRIOT Act]
Available at: http://www.intelligence.senate.gov/nssacl1959.htm
SOTH ANNIVERSARY

USA PATRIOT Improvement and Reauthorization Act of 2005
Available at: http://www.justice.gov/olp/pdf/usa_patriot_improvement_and_reau-
thorization_act.pdf

Protect America Act of 2007
Available at: http://www.intelligence.senate.gov/laws/pl11055.pdf

United States Code, Title 28, section 535 (reporting crimes by Federal officials)
Available at: http://www.law.cornell.edu/uscode/text/28/535

Attorney General’s “Guidelines Regarding Prompt Handling of Reports of Possible
Criminal Activities Involving Foreign Intelligence Sources” (2002)
Available at: https://www.cdt.org/security/ussapatriot/020923guidelines905b.pdf

Attorney General’s “Guidelines for Disclosure of Grand Jury and Electronic, Wire, and
Available at: http://www.fas.org/irp/agency/doj/ag203guidelines.pdf

Attorney General’s “Guidelines Regarding Disclosure to the Director of Central Intelli-
gence and Homeland Security Officials of Foreign Intelligence Acquired in the Course
of a Criminal Investigation” (2002)
Available at: http://old.cdt.org/security/ussapatriot/020923guidelines905a.pdf

United States Code, Title 18, section 1385 (Posse Comitatus Act)
Available at: http://www.law.cornell.edu/uscode/text/18/1385

“National Security Investigations and Prosecutions” David S. Kris and J. Douglas Wil-
son (2007).

In re Sealed Case Nos. 02-001, 319 F.3d 717 (FISA Ct. Rev 2002) (per curiam)
Available at: http://www.fbdlaw.com/Attachments/zail/In%20re%20Sealed%20Case.pdf

Articles on IC Reform Post-9/11


John D. Negroponte & Edward M. Wittenstein, “Urgency, Opportunity, and Frustr-
tation: Implementing the Intelligence Reform and Terrorism Prevention Act of
org/28-2/urgency-opportunity-and-frustration-implementing-the-intelligence-
reform-and-terrorism-preventi
ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

Protection of Intelligence Sources and Methods

• Classification
  * Dept. of Navy v. Egan, 484 US 518 (1988)—holding that the Merit Systems Protection Board does not have the power to overturn an executive branch decision to strip someone of their security clearance. Available at: http://supreme.justia.com/cases/federal/us/484/518/case.html
  * Greene v. McElroy, 360 U.S. 474 (1959)—holding that the government may not deprive a private citizen of a security clearance without providing for confrontation and cross-examination. Available at: http://supreme.justia.com/cases/federal/us/360/474/

• Espionage

• CIPA
  * CIPA Statute—Public Law 96-456. Available at: http://www.law.cornell.edu/uscode/html/uscode18a/uscode_sup_05_18_10_sq5.html
  * United States v. Yunis, 867 F.2d 617 (D.C. Cir. 1989)—explains CIPA as a procedural tool. Available at: http://law.justia.com/cases/federal/appellate-courts/F2/924/1086/224419/
  * United States v. Moussaoui, 382 F.3d 453 (4th Cir. 2004)—one of the defining terrorism prosecutions of the post 9/11 world. Available at: http://law.justia.com/cases/federal/appellate-courts/F3/382/453/570538/

• State Secrets Privilege
  * United States v. Reynolds, 345 U.S. 1 (1953)—creation of privilege (and it's a short decision that shouldn't need to be excerpted). Available at: http://supreme.justia.com/cases/federal/us/345/1/case.html
  * Holder Memo on State Secrets—explains when the DOJ can invoke the state secrets privilege. Available at: http://www.scribd.com/doc/32125087/holder-memo
  * United States v. Aref, 533 F.3d 72 (2d Cir. 2008)—good discussion of CIPA vs. state secrets privilege. Available at: http://www.nsldigest.org/Radler_casebrief_clean.pdf
SOUTH ANNIVERSARY

* Leaks


PREPUBLICATION REVIEW


FOIA/SOURCES AND METHODS

I am pleased to be able discuss this very important topic today, and I thank Suzanne Spaulding, Scott Silliman, and John Norton Moore for inviting me to participate. Several disclosures of classified information over the past year have certainly made this subject timely. I should emphasize at the outset that my presentation today does not necessarily reflect the views of the Director of Central Intelligence or the Office of General Counsel.

I suspect that many of us think there is not much to be said about protecting national security that we have not already heard. As we know, the loss of classified information may be a result of espionage, willful leaks to the media and others, or lax security practices. Regardless of cause or motive, the harm to intelligence sources and methods is real.

As this country attempts to fight terrorism and protect lives, critical infrastructure, and other national interests, it is important for the Intelligence Community to collect foreign intelligence information, analyze it, and communicate it to U.S. policymakers in a way that is both timely and meaningful. Policymakers, in turn, have an obligation to keep the American people appropriately informed of information that affects their health, safety, and welfare. Hundreds of millions of taxpayer dollars have been invested in both human and technical collection programs to provide policymakers with the critical intelligence they need to formulate and implement U.S. policy. The compromise of collection efforts and the failure to protect the sources and methods of collection have resulted in severe and, in some cases, irreparable damage to our collection efforts.

At the core of the debate over how to protect secrets is the need to balance two separate public interests: the public interest in protection -- that is, our national security interests -- and a public interest in disclosure. This is often cast in terms of First Amendment considerations. Some take an absolutist view of the First Amendment; others say the Constitution is not a suicide pact. Regardless, many would agree on at least some elements of the law, but disagree on the policy; others would agree on policy, but not on how to apply the law.

Today, the Intelligence Community is working very closely with other agencies, the private sector, and state and local authorities to balance these interests to support homeland
security efforts. We are developing communications systems that will permit increased information sharing with non-traditional consumers of intelligence. Longstanding impediments to information-sharing are being overcome. Intelligence information is going, must go, not only to traditional defense and foreign policy consumers, but to law enforcement and other civilian agencies to protect our homeland. Some of that information must be made available publicly if policymakers are to warn the American public of terrorist threats. Color-coded warning notices may sound hokey, but there must be a way to communicate important threat information effectively, whether to authorized officials or to the public at large.

I hope no one would suggest that all information related to these threats must be made public indiscriminately. Premature releases can lead to the release of incomplete or totally misleading information. Also, unauthorized releases disrupt our ability to gather more data about specific threats. For this reason, the Intelligence Community will regularly share information about the threat, but not information that would reveal the sources and methods of our collection of that information. We do not want to stop the flow of important information by revealing precisely how we got it.

Yet, often, this is exactly the kind of information revealed through public accounts by government officers, employees, or others who have had privileged access to it. Some would attempt to portray these persons, and the media who report the information, merely as concerned and well-intentioned citizens exercising their First Amendment rights. As then-Secretary of Defense William Cohen stated in September, 2001:

"The romantic notion that most leakers are earnest civil servants driven by conscience is touchingly naive. Most, in fact, are midlevel career or political appointees seeking bureaucratic advantage in the daily battles over making and implementing government decisions."

These remarks were made in connection with the leaks legislation, vetoed by President Clinton, that was included in the fiscal year 2001 Intelligence Authorization Act.

There were several reasons for the veto, and the President asked for a more narrowly drawn bill that would be subjected to the kind of public debate that had no occurred prior to passage of the provision. I think it is particularly instructive to note the following remarks from the President's veto message:

"Unauthorized disclosures damage our intelligence relationships abroad, compromise intelligence gathering, jeopardize lives, and increase the threat of terrorism....those who disclose classified information inappropriately thus commit a gross breach of the public trust and may recklessly put our national security at risk. To the extent that existing sanctions have proven insufficient to address and deter unauthorized disclosures, they should be strengthened. What is in dispute is not the gravity of the problem, but the best way to respond to it."

In looking at possible responses, the interagency recommendations to President Reagan in the 1982 so-called "Willard Report" provide a useful point of departure. That report
recommended action to address unauthorized disclosures administratively and proposed a simple legislative solution to strengthen existing criminal statutes; that is, cover the intentional, unauthorized disclosure of classified information by one person with authorized access to that information, to another person, not a government employee, without such authorized access. For several reasons, that legislative effort died, as have several subsequent efforts including the fiscal year 2001 intelligence bill very similar to the Willard proposal.

It should come as no surprise, as we read the report the Attorney General submitted to Congress last month, that some of those specific recommendations also can be found among the recurring proposals suggested for decades: namely, change cultural attitudes and discipline, enhance internal controls, establish better training programs, classify less information, undertake aggressive investigations, report criminal activity to law enforcement, prosecute where leakers can be identified, establish policies for contacts with the media, enhance authorities of the Director of Central Intelligence to protect sources and methods, and establish liquidated damage provisions in non-disclosure agreements, for example.

I find several recommendations and shifts in emphasis proposed in the Attorney General’s report very important and helpful to build upon ongoing efforts. These include the need for the Department of Justice to review its legal authorities, policies and practices to determine their adequacy to assist in identifying leakers. And, despite the report’s conclusion that the Executive branch should not focus its attention on pursuing new legislation at this time, those who favor leaks legislation should be encouraged by language in the report that recognizes there may be some benefit from a new comprehensive criminal statute and that we “should continue to explore what additional specific steps are needed to strengthen the ability of the United States government to combat unauthorized disclosures of classified information, to include continued consideration of various legislative options.”

What, then, should we do? First, we must aggressively pursue the recommendations of the Attorney General and take a comprehensive approach to improve our own processes and practices: review current policies and authorities, including Executive Order 12958, which governs the classification of information, improve our internal security practices, train our personnel and emphasize personal accountability, establish sensible policies for dealing with the media, and make better use of analytic capabilities as well as technology to track information, identify leakers, and protect intelligence from inadvertent as well as intentional compromise.

Consistent with these and other recommendations, an interagency group within the Intelligence Community over a year ago made several proposals that were put on hold pending completion of the Attorney General’s review. Those proposals are awaiting the DCI’s review. In addition, the DCI has established a special security center to better ensure compliance with security policies across the Intelligence Community, particularly with respect to compartmented intelligence information.

We should also, however, take steps to enact legislation that strengthens our ability to protect classified information. It is important for me to emphasize that I agree leaks legislation alone will not solve our problems. Certainly, the government must improve how it protects its information. However, the Attorney General stated that legislation on the books today may be
used if the facts warrant to prosecute those who violate the trust we place in them. If they can be found. Those laws, however, are primarily addressed at espionage (sections 793 and 794 of title 18) and theft of government property (section 641). We also may use current statutes to prosecute the communication of diplomatic codes and correspondence (section 952), communication of classified information to agents of foreign powers (section 783), disclosure of classified information concerning communications intelligence activities (section 798), and the identities of certain undercover officers and covert human agents (section 421 of title 50). I should also note that it is a crime for government officials and contractors to remove and retain documents or materials containing classified information (section 1924).

There are laws that criminalize disclosures by public officials of crop information (section 1902) and confidential trade secrets and statistics (section 1905). I think national security information deserves no less protection. The benefits from a comprehensive leaks statute, as opposed to one that primarily addresses espionage, would not be guaranteed, but they could be dramatic. It is time for a change.

For example, we need comprehensive leaks legislation for disclosure of sensitive information where the unauthorized recipient is not an agent of a foreign power. It is difficult, psychologically, to generate enthusiasm for investigating and prosecuting so-called “friendly leakers” under espionage laws. Nor should the government have to rely on laws that govern stolen property, or strain to characterize information as “related to national defense.” Also, the government should not have to confirm or reveal secrets in order to punish an employee who has intentionally revealed classified information without authority in violation of the public trust. These factors can dampen the enthusiasm of even the most eager investigators. Yes, current laws may be applied today, but I think carefully drafted laws that target leakers would empower law enforcement investigators by providing a more realistic ability to prosecute and, therefore, to identify those leakers for prosecution. I recognize identification of leakers will not be easy without more, however.

Critics of comprehensive leaks legislation would say that the government classifies too much information. That may be so, but this should not be a defense to a violation of the public trust by persons who have released sensitive information they agreed to protect. Moreover, it’s not clear how this should affect our outrage when we see truly sensitive information being released. Others say that we should employ administrative rather than criminal sanctions to discipline leakers, and that we should not enact legislation that would permit prosecution of employees who reveal information that is not shown in open court to cause damage. Others argue that a per se statute would permit prosecution of employees who discuss secrets with their spouses, or who discuss information already in the public domain. I think we, as lawyers, can deal with the drafting concerns.

Still others argue that leaks can and do benefit the public by opening up secret information about proposed government operations to public debate and challenge. This, I think, is the core of the policy as well as legal debate, and I think we must respect the basis for this view. In seeking an appropriate course, the problem is in attempting to impose criminal penalties for conduct so closely tied, as I think professor Lawrence Tribe has discussed, to the flow of ideas. Discussion of content arguably can further public debate and accommodate
exercise of constitutional rights; I find arguments against legislation to protect specific sources and methods far less convincing.

Earlier I characterized the dilemma as the balancing of two different public interests. Many opponents of leaks legislation tend to value only one public interest: disclosure. But these disclosure decisions should not be left to persons who throw the material over the transom; nor should they be left to the press. This is why we elect officials to public office. Information leaked and discussed publicly may often appear innocuous to those outside the government and even to the government official who is the leaker.

I do not accept the proposition that an author should discount a government official's classification decision and thereby reveal to the public the name of an undercover officer, for example, even over the objections of the undercover officer who has personal and professional concerns for his safety and the compromise of operational activity. That is not serving the public interest; that is simply irresponsible, and potentially illegal.

The press clearly has First Amendment rights that affect the government's ability to protect information that we might all agree should not be disclosed. In law, however, there are limits on what some may consider First Amendment rights. Non-disclosure agreements are one example. Also, it is often policy, not law, that precludes tracing phone calls, issuing search warrants, or convening grand juries to gather data from the press to identify the person, the government employee, who has committed a crime. That policy, as I understand it, requires consultation with the press before issuance of a subpoena. What persons, corporations, or others with information relevant to a criminal investigation would not want that privilege?

Although we will need to be mindful of the competing interests of disclosure and protection, we should not relieve employees of their responsibilities of office. As the Attorney General's report indicates, those who breach their obligations are difficult to identify. I think legislation could help, particularly when the DCI or other officials have exhausted their administrative avenues because they lack the legal authority to investigate across agency lines.

Where, then, does this leave us?

First, of course, the government should review its policies and practices as recommended by the Attorney General. In particular, we need to rethink the policies I have just mentioned for dealing with the press. In addition, new criminal legislation should take a simple, Willard, per se approach and address the following key elements:

- Willful disclosure of classified information;
- To persons not authorized to receive it;
- By persons entrusted with that information;
- If they have reason to believe the information is classified.

Disclosure of information known to be marked classified should be a per se violation, without any requirement that the government separately show damage to the national defense.
To enable the government to investigate leaks more effectively than we can today, I offer the following personal thoughts for discussion in addition to what I have already suggested:

- We should explore options for comprehensive legislation that applies to persons with authorized access, but also applies to disclosures by members of the press and others who engage in a pattern and practice of disclosure, similar to what we have in the Identities Act.

- We should consider legislation applicable to anyone, including the press, who reveals classified information with a gross or reckless disregard of the damage to sources and methods that disclosure could cause. Such legislation affecting the press could require the government to show of damage to allay at least some of the legal concerns.

- The legislation could impose either criminal or civil penalties, including penalties against either the responsible individuals or the corporate giants who are complicit.

- Finally, government agencies should have administrative subpoena authority to obtain information from employees as well as the media, perhaps with the caveat that no information gathered from the media through this process could be used against that media person or organization. Also, the evidence gathered from the press could be limited to use in administrative proceedings against the leaker.

Obviously I am not sympathetic to the view that the First Amendment protects all disclosures that harm the national security, or that the government’s hands should be tied unnecessarily in conducting its investigations. I recognize and embrace the need for public debate of important national issues, but I abhor the loss of vital secrets.

This is a difficult problem, and I do not presume to think I have the silver bullet that will either stop these losses or lead to the punishment of all those who either willfully or recklessly reveal national secrets. I have offered a few ideas to stimulate our thinking and debate. Unfortunately, part of the problem is that we have simply not been effective in making the case that leaking classified information is a crime that should invite penalties like other criminal conduct. I believe a full and open debate over the nature of the problem and specific, aggressive remedies can help. Thank you.
LAWFARE

HARD NATIONAL SECURITY CHOICES

Remarks of CIA General Counsel Stephen Preston at Harvard Law School

By Benjamin Wittes
Tuesday, April 10, 2012 at 1:00 PM

CIA General Counsel Stephen is giving the following remarks today at Harvard Law School:

Remarks of
The Honorable Stephen W. Preston
General Counsel
Central Intelligence Agency
Harvard Law School
Cambridge, Massachusetts
Tuesday, April 10, 2012

"CIA and the Rule of Law"

AS PREPARED FOR DELIVERY

For those working at the confluence of law and national security, the President has made clear that ours is a nation of laws and that an abiding respect for the rule of law is one of our country’s greatest strengths, even against an enemy with only contempt for the law. This is so for the Central Intelligence Agency no less than any other instrument of national power engaged in the fight against al-Qaeda and its militant allies or otherwise seeking to protect the United States from external adversaries. And that is the central point of my remarks this afternoon: Just as ours is a nation of laws, the CIA is an institution of laws and the rule of law is integral to Agency operations.

Before we get to the rule of law, I want to spend a moment on the business of the CIA.

I will start off with two observations that I think are telling:

First, the number of significant national security issues facing our country may be as great today as it has ever been. Just think of what the President and his national security team confront every day: the ongoing threat of terrorist attack against the homeland and U.S. interests abroad; war in Afghanistan and, until recently, Iraq; complex relations with countries like Pakistan and India; the challenges presented by Iran and North Korea; the emergence of China and its growing economic and military power; the growing number of computer network attacks originating outside the United States; profound change in the most volatile area of the world, the greater Middle East, with new regimes in Tunisia, Egypt, and Libya, and continuing violence in Syria; the financial challenges faced by countries in the Euro zone; and the violence associated with drug trafficking in this hemisphere. And the list could go on.

Second, the national security issues facing our country today tend to be intelligence-intensive. Intelligence is fundamental to the efforts of policymakers to come to grips with nearly all of the issues I have just listed — whether international terrorism, the proliferation of Weapons of Mass Destruction, the conduct of non-state actors and rogue states outside the community of nations, cyber security, or the rise of new powers. The nation’s leaders cannot fully understand these issues or make informed policy on these issues without first-rate intelligence.

Putting these two dynamics together — the multitude of different national security issues and the fact that intelligence is critical to almost all of them — it may be that intelligence has never been more important than it is today. At the very least, the intel business is booming.

So what does the CIA do? Our work boils down to three jobs. To quote from the National Security Act of 1947:

• Agency officers, quote, “collect intelligence through human sources and by other appropriate means.” This is also referred to as foreign intelligence collection or, at times, espionage.
• Agency analysts, quote, “correlate and evaluate intelligence related to the national security and provide appropriate dissemination of such intelligence.” This is also referred to as all-source analysis and national intelligence reporting, and it requires that the products of all intelligence disciplines be integrated.
• And the Agency performs such other functions and duties as the President may direct, which may include activities to influence conditions abroad, quote, “where it is intended that the role of the U.S. Government will not be apparent or acknowledged publicly.” In other words, covert action.
If that is, in essence, the business of the CIA, what about the rule of law? And, in particular, why do I say that the rule of law is integral to Agency operations? The answer is that all intelligence activities of the Agency must be properly authorized pursuant to, and must be conducted in accordance with, the full body of national security law that has been put in place over the six-plus decades since the creation of the CIA. And all such activities are subject to strict internal and external scrutiny. This breaks down into three propositions:

First, all intelligence activities of the Agency must be properly authorized pursuant to the law. In this respect, the constraints on the Agency exceed those on virtually any organization in the private sector. A business enterprise is free to do whatever it wants in pursuit of profit, shareholder value, or what-have-you, provided it does not violate the proscriptions of positive law. By contrast, the CIA cannot do anything without an affirmative grant of legal authority to engage in that activity. In some cases, such as foreign intelligence collection, the grant may be broad; in others, such as covert action, the grant of authority might be quite narrow and specific, and subject to numerous conditions. In any event, before any step is taken, the threshold question asked when considering a contemplated activity is, do we have the legal authority to act?

Second, all intelligence activities of the Agency must be conducted in accordance with the law. Assuming there is legal authority to act in the first place, all steps taken must comply with applicable prohibitions and limitations embodied in the United States Constitution, federal statutes, Executive Orders and other Presidential directives, and Agency regulations. To single out some of them:

- The first, fourth, and fifth amendments to the Constitution, which protect the rights of American citizens and certain others.
- The National Security Act of 1947 and the Central Intelligence Agency Act of 1949, which establish the CIA, define its missions, and delineate its role within the Intelligence Community— including the so-called “law enforcement provision,” which bars the Agency from exercising law enforcement powers or performing internal security functions.
- Executive Order 12333, Attorney General-approved guidelines and internal Agency regulations, which contain a host of restrictions on intelligence activities in general and those of the CIA in particular, including the assassination ban in Executive Order Twelve-Three-Three. These directives include numerous provisions intended to protect privacy and civil liberties, including a prohibition against collection in the United States for the purpose of acquiring information on the domestic activities of U.S. Persons; limitations on acquisition, retention and use of information about U.S. Persons; conditions on arrangements with U.S. institutions of higher learning; and conditions on unwritten use of U.S. Persons in intelligence activities and undisclosed participation in organizations in the United States.
- And, finally, the Foreign Intelligence Surveillance Act and the FISA Amendments Act, which govern certain activities in the nature of electronic surveillance and physical searches.

Beyond all these, international law principles may be applicable, as well, and I will come back to this later.

Third, all intelligence activities of the Agency are subject to strict internal and external scrutiny.

It is true that a lot of what the CIA does is shielded from public view, and for good reason: much of what the CIA does is a secret. Secrecy is absolutely essential to a functioning intelligence service, and a functioning intelligence service is absolutely essential to national security, today no less than in the past. This is not lost on the federal judiciary. The courts have long recognized the state secrets privilege and have consistently upheld its proper invocation to protect intelligence sources and methods from disclosure. Moreover, federal judges have dismissed cases on justiciability or political question grounds, acknowledging that the courts are, at times, institutionally ill-equipped and constitutionally incapable of reviewing national security decisions committed to the President and the political branches.

While public and judicial scrutiny may be limited in some respects, it simply does not follow that Agency activities are immune from meaningful oversight. First, there is direct supervision by the National Security Council and the President, who, after all, not only is constitutionally responsible for keeping the American people safe, but also, quote, “shall take Care that the Laws be faithfully executed.” Beyond that, consider this catalog of Agency overseers:

- The intelligence oversight committees of the Senate and House of Representatives. We are bound by statute to ensure that these two committees are kept, quote, “fully and currently informed” with respect to the entire range of intelligence activities, including covert action. They are afforded visibility into late Agency operations that far exceeds the usual scope of congressional oversight of federal agencies. Think about this: during the last Congress, the Agency made, on average, more than two written submissions and two live appearances per day, 365 days a year.
- The Foreign Intelligence Surveillance Court, comprised of Article III judges, provides judicial supervision with respect to certain activities in the nature of electronic surveillance and physical searches.
- The President’s Intelligence Advisory Board, an independent component of the Executive Office of the President, reviews and assesses the performance of the CIA and other elements of the Intelligence Community.
- The Intelligence Oversight Board is a committee of the President’s Intelligence Advisory Board to which the CIA reports apparent legal violations and other significant or highly sensitive matters that could impugn the integrity of the Intelligence Community.
- The Office of the Director of National Intelligence and, now within the past year, the Inspector General for the Intelligence Community.
- And the Agency’s own statutorily independent Inspector General — the only other Agency official, after the Director and the General Counsel, nominated by the President and confirmed by the Senate.
- Last, by no means least, there is the U.S. Department of Justice, to which the CIA is required to report all possible violations of federal criminal laws by employees, agents, liaison, or anyone else.

Okay, I have described the legal regime in which CIA operates. Now I would like to illustrate how the law is applied in practice, by reference to a hypothetical case.
Suppose that the CIA is directed to engage in activities to influence conditions abroad, in which the hand of the U.S. Government is to remain hidden, — in other words covert action — and suppose that those activities may include the use of force, including lethal force. How would such a program be structured so as to ensure that it is entirely lawful? Approaches will, of course, vary depending on the circumstances — there is no single, cookie-cutter approach — but I conceive of the task in terms of a very simple matrix. First is the issue of whether there is legal authority to act in the first place. Second, there is the issue of compliance with the law in carrying out the action. For each of these issues, we would look first, and foremost, to U.S. law. But we would also look to international law principles. So envision a four-box matrix with “U.S. Law” and “International Law” across the top, and “Authority to Act” and “Compliance in Execution” down the side. With a thorough legal review directed at each of the four boxes, we would make certain that all potentially relevant law is properly considered in a systematic and comprehensive fashion.

Now, when I say “we,” I don’t mean to suggest that these judgments are confined to the Agency. To the contrary, as the authority for covert action is ultimately the President’s, and covert action programs are carried out by the Director and the Agency at and subject to the President’s direction, Agency counsel share their responsibilities with respect to any covert action with their counterparts at the National Security Council. When warranted by circumstances, we — CIA and NSC — may refer a legal issue to the Department of Justice. Or we may solicit input from our colleagues at the Office of the Director of National Intelligence, the Department of State, or the Department of Defense, as appropriate.

Getting back to my simple matrix ...

(1) Let’s start with the first box: Authority to Act under U.S. Law.

First, we would confirm that the contemplated activity is authorized by the President in the exercise of his powers under Article II of the U.S. Constitution, for example, the President’s responsibility as Chief Executive and Commander-in-Chief to protect the country from an imminent threat of violent attack. This would not be just a one-time check for legal authority at the outset. Our hypothetical program would be engineered so as to ensure that, through careful review and senior-level decision-making, each individual action is linked to the imminent threat justification.

A specific congressional authorization might also provide an independent basis for the use of force under U.S. law.

In addition, we would make sure that the contemplated activity is authorized by the President in accordance with the covert action procedures of the National Security Act of 1947, such that Congress is properly notified by means of a Presidential Finding.

(2) Next we look at Authority to Act with reference to International Law Principles.

Here we need look no further than the inherent right of national self-defense, which is recognized by customary international law and, specifically, in Article 51 of the United Nations Charter. Where, for example, the United States has already been attacked, and its adversary has repeatedly sought to attack since then and is actively plotting to attack again, then the United States is entitled as a matter of national self-defense to use force to disrupt and prevent future attacks.

The existence of an armed conflict might also provide an additional justification for the use of force under international law.

(3) Let’s move on to Compliance in Execution under U.S. Law.

First, we would make sure all actions taken comply with the terms dictated by the President in the applicable Finding, which would likely contain specific limitations and conditions governing the use of force. We would also make sure all actions taken comply with any applicable Executive Order provisions, such as the prohibition against assassination in Twelve-Triple-Three. Beyond Presidential directives, the National Security Act of 1947 provides, quote, “[a] Finding may not authorize any action that would violate the Constitution or any statute of the United States.” This crucial provision would be strictly applied in carrying out our hypothetical program.

In addition, the Agency would have to discharge its obligations under the congressional notification provisions of the National Security Act to keep the intelligence oversight committees of Congress “fully and currently informed” of its activities. Picture a system of notifications and briefings — some verbal, others written; some periodic, others event-specific; some at a staff level, others for members.

(4) That leaves Compliance in Execution with reference to International Law Principles.

Here, the Agency would implement its authorities in a manner consistent with the four basic principles in the law of armed conflict governing the use of force: Necessity, Distinction, Proportionality, and Humanity. Great care would be taken in the planning and execution of actions to satisfy these four principles and, in the process, to minimize civilian casualties.

So there you have it: four boxes, each carefully considered with reference to the contemplated activity. That is how an Agency program involving the use of lethal force would be structured so as to ensure that it satisfies applicable U.S. and international law.

Switching gears, let us consider a real world case in point: the operation against Osama bin Laden in Abbottabad, Pakistan, on May 2nd [local time]. My purpose is not to illustrate our hypothetical program, but to show that the rule of law reaches the most sensitive activities in which the Agency is engaged.

The bin Laden operation was, of course, a critically important event in the fight against al-Qa’ida. Much has been said and written about the operation in this regard, and I won’t dwell on it now. Rather, I want to focus on the legal aspect of the operation. But if you will indulge me there are a few other aspects of this historic event that warrant mention up front.

First, finding bin Laden was truly a triumph of intelligence. It’s a long story — too long to tell here — but it begins nine years earlier, with the nom de guerre of an al-Qaeda courier. Through painstaking collection and analysis over several years, the Agency and its partners in the Intelligence Community determined his true name. Finding the courier and then his residence in Abbottabad took another year of hard work. Instead of a small house from which the Agency hoped to follow him to bin Laden, the Abbottabad compound suggested immediately the possibility that bin Laden was living there. Extraordinarily high walls, barbed wire, no telephone or internet service, trash burned instead of put out for collection like everybody else’s, children not going to school. Then we learned that an additional family matching the expected profile of bin Laden’s family in flight was living at the compound, never left it, and was unknown to the neighbors. And we learned that the courier was, nine years later, still working for al-Qaeda. It all added up — the only conclusion that made sense of it all was that bin Laden was there. But there was no positive ID.

Which leads to the next point: This was also an example of difficult and momentous Presidential decision-making. There was strong circumstantial evidence that bin Laden was there, but not one iota of direct evidence. No eyes-on identification. And the risks and potential consequences of conducting an operation deep inside Pakistan were enormous, particularly if the operation failed. The President made a sound decision and, in my mind, a gutsy decision.

And, finally, the operation itself was a great triumph for our military. More dramatic than any work of fiction: the tension at the outset, the sickening feeling when one of the helos went down, the seeming immensity waiting to find out if the objective was achieved, and the relief when the last helo lifted off with the force unharmed. My hat’s off to these Special Unit operators — incredibly professional. When the helos went down, they didn’t skip a beat. They had trained for all contingencies and slipped right into Plan B. Then there’s the guy first in the room with bin Laden. Charged by two young women. Trained to expect suicide bombers in these circumstances. He grabbed them, shoved them into a corner and threw himself on top of them, shielding them from the shooting and shielding the guys behind him from the blast if they detonated. His quick thinking, and raw bravery, saved two lives that did not have to end that night.

I am sure the role of the lawyers is not the first thought to come to mind when you think of the bin Laden operation. Admittedly, it may not be the most fascinating aspect, but it is illustrative of the careful attention to the law brought to bear on our country’s most sensitive counterterrorism operations.

Because of the paramount importance of keeping the possibility that bin Laden had been located a secret and then of maintaining operational security as the Abbottabad raid was being planned, there were initially very few people in under the tent. So I cannot say the operation was heavily lawyered, but I can tell you it was thoroughly lawyered. From a legal perspective, this was like other counterterrorism operations in some respects. In other respects, of course, it was extraordinary. What counsel concentrated on were the law-related issues that the decision-makers would have to decide, legal issues of which the decision-makers needed to be aware, and lesser issues that needed to be resolved. By the time the forces were launched, the U.S. Government had determined with confidence that there was clear and ample authority for the use of force, including lethal force, under U.S. and international law and that the operation would be conducted in complete accordance with applicable U.S. and international legal restrictions and principles.

As a result, the operation against bin Laden was not only militarily successful and strategically important, but also fully consistent with all applicable law.

* * *

When I talk about CIA and the rule of law, I speak of the business of the Agency and sometimes draw an analogy between the Agency and a regulated business – a rule-bound and closely watched business at that. But I have to admit that the analogy is seriously flawed at least one respect: the CIA is not a business enterprise. It is, of course, a secret intelligence service charged with protecting the United States against foreign adversaries. It operates at the very tip of the spear in the fight against al-Qaeda and its affiliates and adherents. The work of the CIA is not measured in dollars. Too often the measure is taken in lives lost — like the seven officers killed a little more than two years ago at a forward operating base in eastern Afghanistan and others whose stars concentrate our Memorial Wall. But the measure is also taken in lives saved, which are countless. As I stand before you, I am deeply grateful for what the good men and women who are the CIA do every day — literally, the sacrifices they make — to keep you and me, and our families, safe and secure. All of us should be.

Thank you very much.
INTELLIGENCE COMMUNITY DIRECTIVE
NUMBER 112

CONGRESSIONAL NOTIFICATION
(EFFECTIVE DATE: 16 NOVEMBER 2011)

A. AUTHORITY: The National Security Act of 1947, as amended (hereinafter, National Security Act); Executive Order 12333, as amended; and other applicable provisions of law.

B. PURPOSE: This Directive establishes Intelligence Community (IC) policy to provide written notification to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence (collectively the "Congressional intelligence committees") in order to keep them fully and currently informed of intelligence activities. This Directive replaces and rescinds Intelligence Community Policy Memorandum 2005-100-3, Reporting of Intelligence Activities to Congress, dated January 10, 2006; Timely Notification of Significant Intelligence Activities, dated 24 March 2009; and Follow-up to Reporting Intelligence Matters to Congress, dated 15 October 2009.

C. APPLICABILITY

1. This Directive applies to the IC, as defined by the National Security Act of 1947, and to elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

2. The Directive does not preclude or alter reporting responsibilities to the President's Intelligence Oversight Board as specified in Executive Order 13462 and any successor thereto.

3. This Directive does not apply to reporting of covert actions to the Congressional intelligence committees, to statutory reporting requirements for IC Inspectors General, or to routine informational briefings.

D. POLICY

1. The IC is committed to full and current notification of all intelligence activities as required by the National Security Act, including significant anticipated intelligence actions, significant intelligence failures, and illegal intelligence activities.

2. The provisions of this Directive shall be interpreted with a presumption of notification in fulfillment of the statutory requirement to keep the Congressional intelligence committees fully and currently informed of all intelligence activities.
3. It is IC policy that IC elements shall, in a timely manner, keep the Congressional intelligence committees fully informed, in writing, of all significant anticipated intelligence activities, significant intelligence failures, significant intelligence activities, and illegal activities.

4. IC element heads are responsible for determining whether an event is reportable under this Directive and are responsible for ensuring that Congress is notified of all intelligence activities in accordance with the provisions of this Directive.

5. Determining whether written notification should be provided of a particular intelligence activity is a judgment based on all the facts and circumstances known to the IC element, and on the nature and extent of previous notifications or briefings to Congress on the same matter. Not every intelligence activity warrants written notification. Facts and circumstances of intelligence activities change over time; therefore, IC elements must continually assess whether there is an obligation to report a matter pursuant to the National Security Act and this Directive.

6. As required by the National Security Act, Congress must receive written notification of significant anticipated intelligence activities and significant intelligence failures. General guidelines for determining the types of intelligence activities that warrant written notification follow:

   a. Significant anticipated intelligence activities include:

      (1) intelligence activities that entail, with reasonable foreseeability, significant risk of exposure, compromise, and loss of human life;

      (2) intelligence activities that are expected to have a major impact on important foreign policy or national security interests;

      (3) an IC element’s transfer, to a recipient outside that IC element, of defense articles, personnel services, or "controlled equipment" valued in excess of $1 million as provided in Section 505 of the National Security Act;

      (4) extensive organizational changes in an IC element;

      (5) deployment of new collection techniques that represent a significant departure from previous operations or activities or that result from evidence of significant foreign developments;

      (6) significant activities undertaken pursuant to specific direction of the President or the National Security Council (this is not applicable to covert action, which is covered by Section 503 of the National Security Act); or

      (7) significant acquisition, reprogramming, or non-routine budgetary actions that are of Congressional concern and that are not otherwise reportable under the National Intelligence Program Procedures for Reprogramming and Transfers.

   b. Significant intelligence failures are failures that are extensive in scope, continuing in nature, or likely to have a serious impact on United States (US) national security interests and include:

      (1) the loss or compromise of classified information on such a scale or over such an extended period as to indicate a systemic loss or compromise of classified intelligence information that may pose a substantial risk to US national security interests;
(2) a significant unauthorized disclosure of classified intelligence information that may pose a substantial risk to US national security interests;

(3) a potentially pervasive failure, interruption, or compromise of a collection capability or collection system; or

(4) a conclusion that an intelligence product is the result of foreign deception or denial activity, or otherwise contains major errors in analysis, with a significant impact on US national security policies, programs, or activities.

7. As a matter of policy, IC elements shall provide Congress written notification of other significant intelligence activities and illegal activities. General guidelines for determining these types of intelligence activities warranting notification follow.

a. Significant intelligence activities include:

(1) substantial changes in the capabilities or known vulnerabilities of US intelligence operations or intelligence systems or resources;

(2) programmatic developments likely to be of Congressional interest, such as major cost overruns, a major modification of, or the termination of a significant contract;

(3) developments that affect intelligence programs, projects, or activities that are likely to be of Congressional concern because of their substantial impact on national security or foreign policy;

(4) the loss of life in the performance of an intelligence activity; or

(5) significant developments in, or the resolution of, a matter previously reported under these procedures.

b. Illegal activities include:

(1) An intelligence activity believed to be in violation of US law, including any corrective action taken or planned in connection with such activity;

(2) Significant misconduct by an employee of an IC element or asset that is likely to seriously affect intelligence activities or otherwise is of congressional concern, including human rights violations; or

(3) Other serious violations of US criminal law by an employee of an IC element or asset, which in the discretion of the head of an IC element warrants congressional notification.

8. Criteria described in Sections D.6 and D.7 above are not exhaustive. The absence of any of these criteria shall not be seen as determinative. Each potential determination shall be addressed on its particular merits. If it is unclear whether a notification is appropriate, IC elements should decide in favor of notification.

E. ROLES AND RESPONSIBILITIES: To ensure full and current written notification of intelligence activities consistent with this Directive, each IC element head shall:

1. Designate as a point of contact a senior official who will have access to all relevant information to assist the IC element head in identifying matters that should be reported and who will be responsible for ensuring that notifications are full and current.
2. Establish, in writing, internal processes that will ensure timely identification and full and current reporting of intelligence activities, consistent with this Directive.

3. Provide the Office of the Director of National Intelligence Office of Legislative Affairs (ODNI/OLA) with a point of contact pursuant to Section E.1 above and a copy of the procedures established pursuant to section E.2 above.

4. Ensure that written notifications required under this Directive are provided promptly upon determination that the intelligence activity should be reported under this Directive and the National Security Act.
   a. Within 14 days of final determination by an IC element head (or designee) that a significant activity should be reported, an IC element shall provide written notification. If a complete written notification is not possible at that time, an IC element may provide preliminary oral notification and a projected time for further or final notification.
   b. Written notifications shall contain a concise statement of the pertinent facts, an explanation of the significance of the intelligence activity, and the role of all departments and agencies involved in the intelligence activity.
   c. Oral notifications shall be followed by a written notification, which shall include, in addition to the information described in Section E.4.b above, the date of the oral notification, the office responsible for the subject of the oral notification, and the Congressional members and staff orally notified.
   d. Notification of routine administrative matters such as reprogrammings, facility lease arrangement and renewals, or contract awards should be made with reference to the element’s established timeline for such issues and consistent with Congressional requirements and budget processes.

5. Coordinate, as appropriate, with any other department, agency, or other entity of the US Government involved in the intelligence activity to ensure that an intelligence activity is fully and currently reported to the Congressional intelligence committees.

6. Conduct annual training for element personnel involved in intelligence activities regarding the IC’s obligation to provide information to Congress under the National Security Act and this Directive.

7. Provide the ODNI/OLA copies of all Congressional notifications at the time they are provided to Congress, and a summary of any oral notification.

F. COORDINATION WITH THE DEPARTMENT OF JUSTICE REGARDING CRIMINAL INVESTIGATIONS AND PROSECUTIONS: Where intelligence information subject to this Directive relates to criminal investigations and prosecutions or reasonably anticipated criminal investigations and prosecutions, the IC shall comply with the following procedures:

1. IC elements shall consult with the Attorney General’s designee or designees prior to providing the information to Congressional committees, members, or staff. With respect to the Congressional intelligence committees, this coordination shall ensure that the IC meets its reporting obligations under the National Security Act in a manner consistent with the integrity and independence of criminal investigations and prosecutions.
2. Disagreements between an IC element and the Department of Justice regarding the application of this section will be referred for resolution to the Attorney General and the DNI.

G. LIMITATION: Nothing in this directive shall be construed to limit an IC element’s obligation to report matters to other Congressional committees with oversight jurisdiction or appropriations responsibility for that IC element, subject to the principles identified above regarding criminal matters or potential criminal matters.

H. EFFECTIVE DATE: This Directive becomes effective on the date of signature.

[Signature]
Director of National Intelligence

[Date]
16 November 2011
Executive Order 13462 of February 29, 2008

President's Intelligence Advisory Board and Intelligence Oversight Board

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. It is the policy of the United States to ensure that the President and other officers of the United States with responsibility for the security of the Nation and the advancement of its interests have access to accurate, insightful, objective, and timely information concerning the capabilities, intentions, and activities of foreign powers.

Sec. 2. Definitions. As used in this order:

(a) "department concerned" means an executive department listed in section 101 of title 5, United States Code, that contains an organization listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended (50 U.S.C. 401a(4));

(b) "intelligence activities" has the meaning specified in section 3.4 of Executive Order 12333 of December 4, 1981, as amended; and

(c) "intelligence community" means the organizations listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended.

Sec. 3. Establishment of the President's Intelligence Advisory Board. (a) There is hereby established, within the Executive Office of the President and exclusively to advise and assist the President as set forth in this order, the President's Intelligence Advisory Board (PIAB).

(b) The PIAB shall consist of not more than 16 members appointed by the President from among individuals who are not employed by the Federal Government.

(c) The President shall designate a Chair from among the members of the PIAB, who shall convene and preside at meetings of the PIAB, determine its agenda, and direct its work.

(d) Members of the PIAB and the Intelligence Oversight Board (JOB) established in section 5 of this order:

(i) shall serve without any compensation for their work on the PIAB or the JOB; and

(ii) while engaged in the work of the PIAB or the JOB, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government (5 U.S.C. 5701-5707).

(e) The PIAB shall utilize such full-time professional and administrative staff as authorized by the Chair and approved by the President or the President's designee. Such staff shall be supervised by an Executive
Director of the PIAB, appointed by the President, whom the President may designate to serve also as the Executive Director of the IOB.

Sec. 4. Functions of the PIAB. Consistent with the policy set forth in section 1 of this order, the PIAB shall have the authority to, as the PIAB determines appropriate, or shall, when directed by the President:

(a) assess the quality, quantity, and adequacy of intelligence collection, of analysis and estimates, and of counterintelligence and other intelligence activities, assess the adequacy of management, personnel and organization in the intelligence community, and review the performance of all agencies of the Federal Government that are engaged in the collection, evaluation, or production of intelligence or the execution of intelligence policy and report the results of such assessments or reviews:

(i) to the President, as necessary but not less than twice each year; and

(ii) to the Director of National Intelligence (DNI) and the heads of departments concerned when the PIAB determines appropriate; and

(b) consider and make appropriate recommendations to the President, the DNI, or the head of the department concerned with respect to matters identified to the PIAB by the DNI or the head of a department concerned.

Sec. 5. Establishment of Intelligence Oversight Board.

(a) There is hereby established a committee of the PIAB to be known as the Intelligence Oversight Board.

(b) The IOB shall consist of not more than five members of the PIAB who are designated by the President from among members of the PIAB to serve on the IOB. The IOB shall utilize such full-time professional and administrative staff as authorized by the Chair and approved by the President or the President's designee. Such staff shall be supervised by an Executive Director of the IOB, appointed by the President, whom the President may designate to serve also as the Executive Director of the PIAB.

(c) The President shall designate a Chair from among the members of the IOB, who shall convene and preside at meetings of the IOB, determine its agenda, and direct its work.

Sec. 6. Functions of the IOB. Consistent with the policy set forth in section 1 of this order, the IOB shall:

(a) issue criteria on the thresholds for reporting matters to the IOB, to the extent consistent with section 1.7(d) of Executive Order 12333 or the corresponding provision of any successor order;

(b) inform the President of intelligence activities that the IOB believes:

(i)(A) may be unlawful or contrary to Executive Order or presidential directive; and

(B) are not being adequately addressed by the Attorney General, the DNI, or the head of the department concerned; or

(ii) should be immediately reported to the President.

(c) review and assess the effectiveness, efficiency, and sufficiency of the processes by which the DNI and the heads of departments concerned perform their respective functions under this order and report thereon as necessary, together with any recommendations, to the President and, as appropriate, the DNI and the head of the department concerned;

(d) receive and review information submitted by the DNI under subsection 7(c) of this order and make recommendations thereon, including for any needed corrective action, with respect to such information,
and the intelligence activities to which the information relates, as necessary, but not less than twice each year, to the President, the DNI, and the head of the department concerned; and

(e) conduct, or request that the DNI or the head of the department concerned, as appropriate, carry out and report to the IOB the results of, investigations of intelligence activities that the IOB determines are necessary to enable the IOB to carry out its functions under this order.

Sec. 7. Functions of the Director of National Intelligence. Consistent with the policy set forth in section 1 of this order, the DNI shall:

(a) with respect to guidelines applicable to organizations within the intelligence community that concern reporting of intelligence activities described in subsection 6(b)(i)(A) of this order:

(i) review and ensure that such guidelines are consistent with section 1.7(d) of Executive Order 12333, or a corresponding provision of any successor order, and this order; and

(ii) issue for incorporation in such guidelines instructions relating to the format and schedule of such reporting as necessary to implement this order;

(b) with respect to intelligence activities described in subsection 6(b)(i)(A) of this order:

(i) receive reports submitted to the IOB pursuant to section 1.7(d) of Executive Order 12333, or a corresponding provision of any successor order;

(ii) forward to the Attorney General information in such reports relating to such intelligence activities to the extent that such activities involve possible violations of Federal criminal laws or implicate the authority of the Attorney General unless the DNI or the head of the department concerned has previously provided such information to the Attorney General; and

(iii) monitor the intelligence community to ensure that the head of the department concerned has directed needed corrective actions and that such actions have been taken and report to the IOB and the head of the department concerned, and as appropriate the President, when such actions have not been timely taken; and

(c) submit to the IOB as necessary and no less than twice each year:

(i) an analysis of the reports received under subsection (b)(i) of this section, including an assessment of the gravity, frequency, trends, and patterns of occurrences of intelligence activities described in subsection 6(b)(i)(A) of this order;

(ii) a summary of direction under subsection (b)(iii) of this section and any related recommendations; and

(iii) an assessment of the effectiveness of corrective action taken by the DNI or the head of the department concerned with respect to intelligence activities described in subsection 6(b)(i)(A) of this order.

Sec. 8. Functions of Heads of Departments Concerned and Additional Functions of the Director of National Intelligence.

(a) To the extent permitted by law, the DNI and the heads of departments concerned shall provide such information and assistance as the PIA and the IOB may need to perform functions under this order.

(b) The heads of departments concerned shall:

(i) ensure that the DNI receives:
(A) copies of reports submitted to the IOB pursuant to section 1.7(d) of Executive Order 12333, or a corresponding provision of any successor order; and

(B) such information and assistance as the DNI may need to perform functions under this order; and

(ii) designate the offices within their respective organizations that shall submit reports to the IOB required by Executive Order and inform the DNI and the IOB of such designations; and

(iii) ensure that departments concerned comply with instructions issued by the DNI under subsection 7(a)(ii) of this order.

(c) The head of a department concerned who does not implement a recommendation to that head of department from the PIAB under subsection 4(b) of this order or from the IOB under subsections 6(c) or 6(d) of this order shall promptly report through the DNI to the Board that made the recommendation, or to the President, the reasons for not implementing the recommendation.

(d) The DNI shall ensure that the Director of the Central Intelligence Agency performs the functions with respect to the Central Intelligence Agency under this order that a head of a department concerned performs with respect to organizations within the intelligence community that are part of that department.

Sec. 9. References and Transition. (a) References in Executive Orders other than this order, or in any other presidential guidance, to the "President's Foreign Intelligence Advisory Board" shall be deemed to be references to the President's Intelligence Advisory Board established by this order.

(b) Individuals who are members of the President's Foreign Intelligence Advisory Board under Executive Order 12863 of September 13, 1993, as amended, immediately prior to the signing of this order shall be members of the President's Intelligence Advisory Board immediately upon the signing of this order, to serve as such consistent with this order until the date that is 15 months following the date of this order.

(c) Individuals who are members of the Intelligence Oversight Board under Executive Order 12863 immediately prior to the signing of this order shall be members of the Intelligence Oversight Board under this order, to serve as such consistent with this order until the date that is 15 months following the date of this order.

(d) The individual serving as Executive Director of the President's Foreign Intelligence Advisory Board immediately prior to the signing of this order shall serve as the Executive Director of the PIAB until such person resigns, dies, or is removed, or upon appointment of a successor under this order and shall serve as the Executive Director of the IOB until an Executive Director of the IOB is appointed or designated under this order.

Sec. 10. Revocation. Executive Order 12863 is revoked.

Sec. 11. General Provisions.

(a) Nothing in this order shall be construed to impair or otherwise affect:

(i) authority granted by law to a department or agency, or the head thereof; or

(ii) functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) Any person who is a member of the PIAB or IOB, or who is granted access to classified national security information in relation to the activities of the PIAB or the IOB, as a condition of access to such information, shall sign and comply with the agreements to protect such information from unauthorized disclosure. This order shall be implemented in a manner consistent with Executive Order 12958 of April

(c) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(d) 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.

[signed:] George W. Bush

THE WHITE HOUSE,

February 29, 2008.
Department of Defense

DIRECTIVE

NUMBER 5143.01
November 23, 2005

SUBJECT: Under Secretary of Defense for Intelligence (USD(I))

References: (a) Title 10, United States Code
(b) Title 50, United States Code
(c) Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," 118 Stat. 3638, December 17, 2004
(d) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(e) through (ad), see enclosure 1

1. PURPOSE

Under the authorities vested in the Secretary of Defense by reference (a), including Sections 113 and 137, and consistent with reference (b), including Sections 401 through 405, as well as references (c), (d), and Executive Order (E.O.) 13355 (reference (e)), this Directive:

1.1. Assigns the responsibilities, functions, relationships, and authorities of the Under Secretary of Defense for Intelligence (USD(I)).

1.2. Cancels the Secretary of Defense Memorandum, "Office of the Under Secretary of Defense for Intelligence"; the Deputy Secretary of Defense Memorandum, "Implementation Guidance on Restructuring Defense Intelligence—and Related Matters"; and DoD Directive 5134.11 (references (f) through (h)).

1.3. Authorizes the USD(I), as a Principal Staff Assistant (PSA) reporting directly to the Secretary of Defense, to promulgate DoD policy in DoD Instructions within the responsibilities, functions, and authorities assigned herein.

1.4. Shall conform to and be consistent with law and Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI).
2. **APPLICABILITY**

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the “DoD Components”).

3. **DEFINITIONS**

Terms used in this Directive are defined in enclosure 2.

4. **RESPONSIBILITIES AND FUNCTIONS**

The USD(I) is the PSA and advisor to the Secretary and Deputy Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters (hereafter referred to as “intelligence, counterintelligence, and security” matters). In this capacity, the USD(I) exercises the Secretary of Defense’s authority, direction, and control over the Defense Agencies and DoD Field Activities that are Defense intelligence, counterintelligence, or security Components and exercises planning, policy, and strategic oversight over all DoD intelligence, counterintelligence, and security policy, plans, and programs. In the exercise of assigned responsibilities, the USD(I) shall:

4.1. Serve as the senior DoD intelligence, counterintelligence, and security official below the Secretary and Deputy Secretary of Defense.

4.2. Serve as the primary representative of the Secretary of Defense to the Office of the Director of National Intelligence (ODNI) and other members of the Intelligence Community.

4.3. For human capital:

4.3.1. Consistent with DoD Directive 1400.35 (reference (i)), exercise policy oversight of personnel in defense intelligence positions to ensure that Defense intelligence, counterintelligence, and security Components are manned, trained, equipped, and structured to support the missions of the Department and fully satisfy the needs of the Combatant Commands, the Military Departments, and the ODNI, as appropriate.

4.3.2. Develop and oversee the policies associated with the Defense Civilian Intelligence Personnel System in conjunction with the Under Secretary of Defense for Personnel and Readiness pursuant to reference (i).
4.3.3. Develop policy and provide oversight on training, education, and career
development of personnel within the Defense intelligence, counterintelligence, and security
Components and ensure integration of Defense intelligence into other DoD training within the
Department of Defense and Intelligence Community, as appropriate.

4.3.4. Identify candidates for Secretary of Defense consideration to be nominated and/or
appointed to serve as Directors of the Defense Intelligence Agency, the National Geospatial-
Intelligence Agency, the National Reconnaissance Office, and the National Security
Agency/Central Security Service.

4.3.5. Oversee the duty performance of the Directors of the Defense Intelligence
Components (identified in paragraph 5.1.2) and solicit evaluative input from the DNI, as
appropriate.

4.3.6. Oversee the implementation of DoD detailee policy within the Defense
intelligence, counterintelligence, and security Components, and exercise approval authority,
consistent with the processes developed by the Secretary of Defense and the DNI, over the
assignment of intelligence, counterintelligence, and security personnel, including personnel who
are subject to the Defense Civilian Intelligence Personnel System, detailed to duty from one DoD
Component to another or to an external organization. All requests for detailees external to the
Department to perform duties in the fields of intelligence, counterintelligence, or security shall
receive the concurrence of the USD(I) prior to approval by the Director of Administration and
Management pursuant to applicable law, regulations, and policy, including DoD Directive
1000.17 (reference (j)).

4.4. For planning, programming, budgeting, and execution matters, and other budgetary
matters, consistent with Section 135 of 10 U.S.C. (reference (a)):

4.4.1. Participate, pursuant to the responsibilities and functions prescribed herein, in the
DoD Planning, Programming, Budgeting, and Execution (PPBE) process, which includes
proposing DoD resource programs, formulating budget estimates, recommending resource
allocations and priorities, and monitoring the implementation of approved programs in order to
ensure adherence to approved policy and planning guidance. The USD(I) shall consult and
coordinate with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of
Defense (Comptroller) (USD(C)), and the Director, Program Analysis and Evaluation (DPA&E)
on PPBE matters.

4.4.2. Support the Assistant Secretary of Defense for Legislative Affairs and USD(C) in
presenting, justifying, and defending intelligence, counterintelligence, and security programs
and budgets before the Congress as well as evaluating and assessing Congressional activity for
impact on all assigned areas of responsibility, and consult and coordinate with the USD(C) on
budgetary matters, as appropriate, and the DNI on National Intelligence Program (NIP) matters.
4.4.3. Oversee Defense intelligence, counterintelligence, and security policy, plans, programs, required capabilities, and resource allocations, which includes exercising responsibility for the DoD Components within the NIP and the Military Intelligence Program (MIP), according to Deputy Secretary of Defense Memorandum (reference (k)).

4.4.4. Oversee all Defense intelligence budgetary matters to ensure compliance with the budget policies issued by the DNI for the NIP.

4.5. For acquisition matters:

4.5.1. Provide advice and assistance, as appropriate, to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, the Defense Acquisition Board, the Defense Space Acquisition Board, the DNI, and other officials and/or entities in the U.S. Government concerning acquisition programs that significantly affect Defense intelligence, counterintelligence, and security Components as well as intelligence, counterintelligence, and security programs.

4.5.2. Exercise acquisition authority as delegated by the USD(AT&L), the DNI, or other appropriate officials in the U.S. Government for the acquisition of technologies, systems, and equipment.

4.5.3. In coordination with the USD(AT&L), oversee the exercise of acquisition authority by the Directors of the Defense intelligence, counterintelligence, and security Components.

4.6. Provide policy and strategic oversight of all Defense intelligence, counterintelligence, and security programs within the Department of Defense operating under the authority, direction, and control of the USD(I) as prescribed herein, and ensure that these organizations perform their missions.

4.7. Ensure that USD(I) policies and programs are designed and managed to improve standards of performance, economy, and efficiency and that all of the Defense Agencies and DoD Field Activities over which the USD(I) exercises the Secretary of Defense's authority, direction, and control are attentive and responsive to the requirements of their organizational customers, both internal and external to the Department of Defense.

4.8. Serve on boards, committees, and other groups pertaining to assigned responsibilities and functions and represent the Secretary of Defense on all intelligence, counterintelligence, and security matters in other U.S. Government fora.

4.9. For Defense intelligence:
4.9.1. Oversee all DoD intelligence policies and activities, including those implemented pursuant to DoD Directive 5240.1 (reference (l)), and establish priorities to ensure conformance with Secretary of Defense and DNI policy guidance, as appropriate.

4.9.2. Develop, coordinate, and oversee the implementation of DoD policy, strategy, programs, and guidance on manned and unmanned spaceborne, airborne, surface, and subsurface activities and other matters pertaining to intelligence, surveillance, and reconnaissance (ISR), including those in support of foreign and international requirements involving the use of space and non-space resourced ISR activities and products.

4.9.3. Oversee Sensitive Reconnaissance Operations (SRO) Program policy and maintain cognizance of non-SRO reconnaissance and surveillance activities and operations.

4.9.4. Develop and oversee policy for Defense intelligence planning and preparation activities as well as Defense warning and forecasting activities.

4.10. For counterintelligence:

4.10.1. Represent the Secretary of Defense in meetings and communications with the National Counterintelligence Executive (NCIX).

4.10.2. Develop, coordinate, and oversee the implementation of DoD policy, programs, and guidance for DoD counterintelligence pursuant to DoD Directive 5240.2 (reference (m)) and oversee and provide guidance to ensure compliance with counterintelligence policies issued by the DNI, as appropriate.

4.10.3. Oversee DoD polygraph policies and ensure the Department of Defense supports the polygraph requirements identified by the heads of other Federal Agencies with polygraph programs.

4.10.4. Promptly inform the Secretary and Deputy Secretary of Defense, OSD PSAs, Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff as well as the DNI, NCIX, and Congress of significant counterintelligence activity, as appropriate.

4.11. For security policy matters:

4.11.1. Serve as the DoD Senior Security Official pursuant to E.O. 12958 (reference (n)) and advise the Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and the Heads of other DoD Components on the development and integration of risk-managed security and protection policies and programs, except for Nuclear Physical Security pursuant to DoD Directive O-5210.41 (reference (o)).

4.11.2. Develop, coordinate, and oversee the implementation of DoD policy, programs, and guidance for personnel, physical, industrial, information, operations, chemical/biological, and DoD Special Access Program (SAP) security as well as research and technology protection.
4.11.2.1. Oversee the implementation of policy regarding the protection of sensitive compartmented information pursuant to Presidential and DNI guidance as well as DoD Directive 8520.1 (reference (p)).

4.11.2.2. Perform all duties and responsibilities of the Secretary of Defense regarding the National Industrial Security Program pursuant to E.O. 12829 (reference (q)).

4.11.3. Develop and oversee DoD policy regarding the sharing of information consistent with applicable laws, regulations, and policy, including E.O. 12333 (reference (d)), DNI policies, and DoD policies.

4.11.3.1. Ensure that all DoD Components integrate security education and awareness into their personnel-security programs pursuant to E.O. 12968 (reference (r)).

4.11.3.2. Develop and oversee DoD SAP security policy, carry out guidance provided by the DoD SAP Oversight Committee, serve as the oversight authority for all DoD Intelligence SAPs and those SAPs delegated to the USD(I) for oversight, and establish a SAP Coordination Office (SAPCO) in OUSD(I) that provides administrative support to and facilitates the management of SAPs delegated to the USD(I), and ensure that all NIP-funded SAPs are consistent with DNI policies and coordinated with the ODNI.

4.12. Serve as the DoD focal point for all policy and oversight matters relating to intelligence information sharing and interoperability of Defense intelligence systems and processes pursuant to reference (c) and E.O. 13356 and E.O. 13354 (references (s) and (t)). The USD(I) shall develop, coordinate, and oversee DoD requirements and compliance with intelligence information sharing and interoperability requirements and policies issued by the DNI.

4.13. For Information Operations (IO):

4.13.1. Serve as the PSA and advise the Secretary of Defense on development and oversight of DoD IO policy and integration activities, and serve as the DoD lead with the Intelligence Community on DoD IO Issues.

4.13.2. Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, and develop capabilities in support of IO requirements pursuant to DoD Directive S-3600.1 (reference (u)).

4.13.3. Provide IO assessments for Operational Plans and Security Cooperation Guidance in support of the USD(P).

4.15. Pursuant to 10 U.S.C. (reference (a)), 50 U.S.C. (reference (b)), and Secretary of Defense guidance, develop policies and implementation guidance, as well as provide oversight to ensure versatility and agility in meeting the Department's missions.

4.16. Develop, coordinate, and oversee policy and policy implementation for all other sensitive intelligence, counterintelligence, security, and special technology programs and activities within the Department of Defense.

4.17. Identify gaps and opportunities for technology insertion to enhance intelligence, counterintelligence, and security capabilities of the Department and, in conjunction with USD(AT&L), Director of Operational Test and Evaluation, Director of Defense Research and Engineering, and other OSD PSAs, as appropriate, oversee research, development, test, and evaluation, subject to DoD acquisition regulations and Sections 139 and 2399 of 10 U.S.C. (reference (a)). NIP-funded programs shall be undertaken in coordination with the DNI.

4.18. Periodically assess any DoD Executive Agent assignments under the cognizance of the USD(l) for continued need, currency, and effectiveness and efficiency in satisfying end user requirements, consistent with DoD Directive 5101.1 (reference (x)).

4.19. Coordinate with the USD(P) regarding intelligence and intelligence-related matters that affect antiterrorism, counterterrorism, and terrorism consequence management policies as well as special operations intelligence elements and special operations-related activities funded through the MIP.

4.20. Perform such other duties as the Secretary may prescribe.

5. RELATIONSHIPS

5.1. The Under Secretary of Defense for Intelligence, in the performance of assigned functions and responsibilities, shall take precedence in the Department of Defense on all intelligence, counterintelligence, and security matters prescribed herein after the Secretary and Deputy Secretary of Defense, and shall:

5.1.1. Report directly to the Secretary of Defense.

5.1.2. Exercise the Secretary of Defense's authority, direction, and control over:

5.1.2.1. Director, Defense Security Service;

5.1.2.2. Director, DoD Counterintelligence Field Activity;

5.1.2.3. Director, Defense Intelligence Agency;

5.1.2.4. Director, National Geospatial-Intelligence Agency;
5.1.2.5. Director, National Security Agency/Central Security Service;

5.1.2.6. Director, National Reconnaissance Office; and

5.1.2.7. Such other positions and organizations as may be established by the USD(I), consistent with applicable law, within the resources provided by the Secretary of Defense.

5.1.3. Exercise the Secretary of Defense’s authority, direction, and control over the Directors listed in subparagraphs 5.1.2.3 through 5.1.2.6 above, in consultation with the DNI regarding national intelligence and related matters under the purview of the DNI, as appropriate, consistent with Secretary of Defense and DNI responsibilities under 50 U.S.C. (reference (b)) and the “Intelligence Reform and Terrorism Prevention Act of 2004” (reference (c)).

5.1.4. Serve as the Secretary of Defense’s focal point pursuant to responsibilities and functions prescribed herein with other government entities, including the National Security Council, Homeland Security Council, Department of the Treasury, Department of State, Department of Justice, and Department of Homeland Security as well as foreign governments, international organizations, state agencies, the Intelligence Community, and Congress.

5.1.5. As Program Executive for the Military Intelligence Program pursuant to Acting Deputy Secretary of Defense Memorandum (reference (k)), provide policy, guidance, and oversight and establish mechanisms for the appropriate coordination with USD(P), USD(C), DPA&E, and Chairman of the Joint Chiefs of Staff throughout the DoD planning, programming, budgeting, and execution cycles, according to DoD Directive 7045.14 (reference (y)). The USD(I) will work in close concert with the DNI, as appropriate. The USD(I) shall chair or participate in, as appropriate, groups established to address programmatic issues.

5.1.6. Make recommendations to the USD(C) on all transfers, realignments, and/or reprogramming of funds to and from the Military Intelligence Program in accordance with thresholds established in the Financial Management Regulation (reference (z)). The USD(I) shall consult with the ODNI in advance of transferring or reprogramming funds made available under the Military Intelligence Program. In addition, the USD(I) shall coordinate or consult with other OSD PSAs and Heads of the DoD Components, as appropriate, on all reprogramming plans.

5.1.7. For national intelligence centers established by the DNI:

5.1.7.1. Coordinate with the USD(P) as well as the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and other OSD PSAs, as appropriate, to ensure that DoD support to national intelligence centers is provided, as necessary, and comply with DoD Directive 1000.17 (reference (j)), as applicable.

5.1.7.2. Provide policy, oversight, and guidance for all Defense intelligence, counterintelligence, and security support provided to national intelligence centers, including the National Counterterrorism Center and the National Counterproliferation Center as well as similar activities.
5.1.8. Coordinate with the Inspector General of the Department of Defense and the Assistant to the Secretary of Defense for Intelligence Oversight to ensure that Defense intelligence, counterintelligence, and security Components and DoD activities comply with statutory, Executive, Departmental and other national policies, guidance, and regulations.

5.1.9. Work closely with the USD(P) to ensure that space-based-intelligence systems support the Secretary of Defense and his position regarding national security space policy.

5.1.10. Work closely with the DoD Executive Agent for Space regarding his or her DoD-wide responsibilities representing and advocating space interests in the planning and programming processes and Defense acquisition process, pursuant to the DoD Directive 5101.2 (reference (aa)).

5.1.11. Work closely with the Chairman of the Joint Chiefs of Staff in carrying out functions under Section 153 of reference (a) to ensure the development of intelligence, counterintelligence, and security programs that enhance interoperability and effectively support the joint warfighting responsibilities of the Commanders of the Combatant Commands consistent with Sections 164, 167, and 167a of 10 U.S.C. (reference (a)).

5.1.12. Work closely with the DNI to ensure effective, complementary, and mutual support between Defense intelligence programs and the NIP.

5.1.13. Use existing systems, facilities, and services of the Department of Defense and other Federal Agencies, when practicable, to avoid duplication and to achieve maximum readiness, sustainability, economy, and efficiency.

5.1.14. Coordinate and exchange information with other OSD officials and the Heads of the DoD Components having collateral or related responsibilities and functions.

5.2. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, pursuant to DoD Directive 5144.1 (reference (ab)), shall work closely with the USD(I) on all matters prescribed herein, as appropriate.

5.3. The General Counsel of the Department of Defense shall serve as the legal advisor to the Secretary of Defense, the Deputy Secretary of Defense, the USD(I), and other DoD officials, as appropriate, regarding legal matters associated with intelligence, counterintelligence, and security matters and shall consult as appropriate with the USD(I) on such matters.

5.4. The Heads of the Defense Intelligence Components shall ensure, to the extent possible, USD(I) receipt of intelligence estimates or other substantive and time-sensitive intelligence produced by the Defense Intelligence Components and submitted to the Secretary of Defense, Deputy Secretary of Defense, and the Chairman of the Joint Chiefs of Staff as well as the DNI or other senior officials outside of the Department of Defense.
5.5. The other Office of the Secretary of Defense officials and the Heads of the DoD Components shall coordinate with the USD(I) on all matters related to the authorities, responsibilities, and functions assigned in this Directive.

5.6. The Secretaries of the Military Departments shall provide timely advice to the USD(I) and shall ensure that the policies and guidance issued by the USD(I) are implemented in their respective Military Departments.

5.7. The Chairman of the Joint Chiefs of Staff shall consult with, and seek the advice of, the Combatant Commanders on policy, programs, and other related activities that support the Department's intelligence, counterintelligence, and security goals and missions, including requests for advice, resources, assistance, and other functions pursuant to Section 153 of 10 U.S.C. (reference (a)). The Chairman of the Joint Chiefs of Staff shall facilitate communications with the Combatant Commanders to ensure intelligence, counterintelligence, and security interoperability and support for joint warfighting, particularly as they relate to intelligence-related functions prescribed herein and consistent with Sections 164, 167, and 167a of 10 U.S.C. (reference (a)).

6. AUTHORITIES

The USD(I) is hereby delegated authority to:

6.1. Issue in DoD Instructions, DoD policy within the authorities and responsibilities assigned herein, including authority to identify collateral responsibilities of OSD officials and the Heads of the DoD Components. Such instructions shall be fully coordinated in accordance with DoD 5025.1-M (reference (ac)). Further, in areas of assigned responsibilities and functions, the USD(I) has authority to issue other DoD Instructions, DoD Publications, and one-time directive-type memoranda, consistent with reference (ac), that implement policy approved by the Secretary of Defense. Instructions to the Military Departments shall be issued through the Secretaries of the Military Departments. Instructions to the Combatant Commands normally shall be communicated through the Chairman of the Joint Chiefs of Staff.

6.2. Obtain reports and information, consistent with DoD Directive 8910.1 (reference (ad)), as necessary in carrying out assigned responsibilities and functions.

6.3. Communicate directly with the Office of the DNI on Defense intelligence matters on behalf of the Secretary of Defense.

6.4. Communicate directly with the Heads of the DoD Components, as necessary, to carry out assigned functions and responsibilities, including the transmission of requests for advice and assistance. Communications to the Military Departments shall be through the Secretaries of the Military Departments, their designees, or as otherwise provided in law or directed by the Secretary of Defense in other DoD issuances. Communications to the Commanders of the Combatant Commands normally shall be transmitted through the Chairman of the Joint Chiefs of Staff.
6.5. Establish arrangements for DoD participation in U.S. Governmental programs for which the USD(I) is assigned primary DoD cognizance.

6.6. Communicate with other Government officials, representatives of the Legislative Branch, members of the public, and representatives of foreign governments, as appropriate, in carrying out assigned responsibilities and functions.

6.7. Exercise the delegations of authority in enclosure 3.

7. **EFFECTIVE DATE**

This Directive is effective immediately.

Enclosures — 3

E1. References, continued
E2. Definitions
E3. Delegations of Authority
E1. ENCLOSED 1

REFERENCES, continued

(e) Executive Order 13355, "Strengthened Management of the Intelligence Community," August 27, 2004
(f) Secretary of Defense Memorandum, "Office of the Under Secretary of Defense for Intelligence," April 18, 2003 (hereby canceled)
(g) Deputy Secretary of Defense Memorandum, "Implementation Guidance on Restructuring Defense Intelligence—and Related Matters," May 8, 2003 (hereby canceled)
(h) DoD Directive 5134.11, "Defense Airborne Reconnaissance Office (DARO)," April 5, 1995 (hereby canceled)
(k) Acting Deputy Secretary of Defense Memorandum, "Establishment of the Military Intelligence Program," September 1, 2005
(m) DoD Directive 5240.2, "DoD Counterintelligence (CI)," May 22, 1997
(n) Executive Order 12958, "Classified National Security Information," April 17, 1995, as amended
(s) Executive Order 13356, "Strengthening the Sharing of Terrorism Information to Protect Americans," August 27, 2004
(t) Executive Order 13354, "National Counterterrorism Center," August 27, 2004
(w) DCID 5/1, "Coordination of United States Clandestine Foreign Activities Abroad," December 19, 1984
(ab) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer," May 2, 2005

1 If a copy is needed on a need-to-know basis, contact the Office of the Under Secretary of Defense for Intelligence
Staff in the Pentagon at USD/ID.Pubs@osd.mil.
Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City

SECRETARY OF DEFENSE LEON E. PANETTA: Thank you. Thank you very much.

Thank you so much for this wonderful evening and the chance to enjoy such terrific company and be able to express my deepest gratitude to this organization for all of the great things that it does on behalf of those that serve in our military.

Bruce, my greatest thanks to you for your kind remarks and for your leadership here.

And I -- I accept this award, not so much for myself but I accept it on behalf of the men and women in uniform who are putting their lives on the line every night, every day in order to protect this country.

(Applause.)

I want to congratulate the troops from the 82nd, they're -- they're the very best.

I also want to congratulate Frank for receiving this reward, the great service that he does in helping to -- to find jobs for those that are returning so that they can be part of -- of their community after serving this country, to protect their community is outstanding. And besides that, and perhaps most importantly, he's Italian. It's nice to have another Italian honored this evening.

(Applause.)

I also want to thank Fran Townsend. She's a great friend and, obviously, a tremendous Master of Ceremonies this evening. And the reason I -- the reason I asked Fran to serve on the board is because she is bright. She is capable. She's dedicated. She -- she's a straight talker, she knows what she's talking about. She's dedicated to this country and in a room of a lot of ugly old guys, she's not bad to look at.

(Laughter.)

General Meigs, thank you for your leadership as well and for your distinguished service to this country.

I am truly honored to be with you this evening. We gather in the midst of a very important rational contest. It's one that will continue to play out over the coming weeks in unpredictable ways before a final decision is reached. And in fact, some of the key players are dueling tonight.

So I want to be very clear about where my loyalties lie in this contest, I have always been and always will be for the New York Yankees.

(Applause.)

And I think the score is 1-to-1. Right?
In all seriousness, I really do appreciate the opportunity to come back to this great city. This is -- New York is a special place for me and I'll tell you why. I am -- I'm the son of Italian immigrants and both of my parents came through New York, came through Ellis Island like so many millions of others. That made this a special place for me.

I also had the opportunity to be here and work as an Executive Assistant to the Mayor of New York City, a guy named John Lindsey at the time.

I also had the opportunity to work very closely with the delegation in Congress. As a matter of fact, in Washington.

I lived with Chuck Schumer and a group of other members of Congress in what was well known as Animal House in Washington. And you can't live with Schumer and not develop an appreciation for New York City.

I also served on the Board of the New York Stock Exchange for six years. And I was on the board when 9/11 took place and I want you to know how much at that time I appreciated the great courage of the people of New York in the face of that attack. And I remembered that courage when I had a chance to lead the operation that went after Bin Laden.

We sent a very clear message to the world. We sent a very clear message to terrorists that in fact, don't ever attack this country because you will not get away with it.

(Applause.)

I've long appreciated, from my own experience, New York's role as the center of gravity for our nation's economy. This is where it's at. And for that reason, it's an honor to be able to speak before this kind of distinguished audience of business leaders and innovators because you understand what a strong national defense is all about and you understand that a strong national defense and a strong economy go hand in hand.

With that in mind, tonight I'd like to discuss with you an issue that I think is at the very nexus of business and national security: the threats facing the United States in cyberspace and the role that the Defense Department must play in defending this country from those kinds of threats.

We're on an aircraft carrier, a famous and great aircraft carrier and it's a fitting and appropriate venue to have this discussion. This ship and the technology that's on display at this museum, attests to one of the central achievements of the United States in the 20th century, our ability to project power and strength across the land, across the high seas, across the skies and across outer space.

We secured those domains. Securing them helped ensure that they were used to advance peace and prosperity and were not used to promote war and aggression.

It is with that same goal in mind, today we have to address a new domain that we must secure to have peace and prosperity in the world of tomorrow.

Cyberspace has fundamentally transformed the global economy. It's transformed our way of life, providing two billion people across the world with instant access to information to communication, to economic opportunities.

Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers.

The Internet is open. It's highly accessible, as it should be. But that also presents a new terrain for warfare. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens.

I know that when people think of cybersecurity today, they worry about hackers and criminals who prowl the Internet, steal people's identities, steal sensitive business information, steal even national security secrets. Those threats are real and they exist today.

But the even greater danger -- the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states are violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.

Let me give you some examples of the kinds of attacks that we have already experienced.
In recent weeks, as many of you know, some large U.S. financial institutions were hit by so-called Distributed Denial of Service attacks. These attacks delayed or disrupted services on customer websites. While this kind of tactic isn’t new, the scale and speed with which it happened was unprecedented.

But even more alarming is an attack that happened two months ago when a very sophisticated virus called Shamoon infected computers in the Saudi Arabian State Oil Company Aramco. Shamoon included a routine called a ‘wiper’, coded to self-execute. This routine replaced crucial systems files with an image of a burning U.S. flag. But it also put additional garbage data that overwrote all the real data on the machine. More than 30,000 computers that it infected were rendered useless and had to be replaced. It virtually destroyed 30,000 computers.

Then just days after this incident, there was a similar attack on RasGas of Qatar, a major energy company in the region. All told, the Shamoon virus was probably the most destructive attack that the private sector has seen to date.

Imagine the impact an attack like that would have on your company or your business.

These attacks mark a significant escalation of the cyber threat and they have renewed concerns about still more destructive scenarios that could unfold.

For example, we know that foreign cyber actors are probing America’s critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country.

We know of specific instances where intruders have successfully gained access to these control systems.

We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life.

Let me explain how this could unfold. An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches. They could, for example, derail passenger trains or even more dangerous, derail trains loaded with lethal chemicals.

They could contaminate the water supply in major cities or shutdown the power grid across large parts of the country.

The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks.

The collective result of these kinds of attacks could be a cyber Pearl Harbor, an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.

As director of the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East.

And the cyber threats facing this country are growing. With dramatic advances, this is an area of dramatic developments in cyber technology. With that happening, potential aggressors are exploiting vulnerabilities in our security. But the good news is this, we are aware of this potential. Our eyes are wide open to these kinds of threats and we are a nation that, thank God, is on the cutting edge of this new technology. We are the best and we have to stay there.

The Department of Defense, in large part through the capabilities of the National Security Agency, NSA, has develop the world’s most sophisticated system to detect cyber intruders and attackers.

We are acting aggressively to get ahead of this problem, putting in place measures to stop cyber attacks dead in their tracks. We are doing this as part of a broad whole of government effort to confront cyber threats.

The Department of Homeland Security has the lead for domestic cybersecurity, the FBI also has a key part to play and investigating and preventing cyber-attacks. And our intelligence agencies, of course, are focused on this potential threat as well.
The State Department is trying to forge international consensus on the roles and responsibilities of nations to help secure cyberspace.

The Department of Defense also has a role. It is a supporting role but it is an essential role. And tonight I want to explain what that means. But first let me make clear what it does not mean.

It does not mean that the Department of Defense will monitor citizens' personal computers. We're not interested in personal communication or in e-mails or in providing the day to day security of private and commercial networks. That is not our goal. That is not our job. That is not our mission.

Our mission is to defend the nation. We defend. We deter, and if called upon, we take decisive action to protect our citizens. In the past, we have done thorough operations on land and at sea, in the skies and in space. In this century, the United States military must help defend the nation in cyberspace as well.

If a foreign adversary attacked U.S. soil, the American people have every right to expect their national defense forces to respond.

If a crippling cyber attack were launched against our nation, the American people must be protected. And if the Commander in Chief orders a response, the Defense Department must be ready to obey that order and to act.

To ensure that we fulfill our role to defend the nation in cyberspace, the department is focusing on three main tracks.

One, developing new capabilities.

Two, putting in place the policies and organizations we need to execute our mission.

And three, building much more effective cooperation with industry and with our international partners.

Let me briefly talk about each of these.

First, developing new capabilities. DoD is investing more than $3 billion annually in cybersecurity because we have to retain that cutting edge capability in the field.

Following our new defense strategy, the department is continuing to increase key investments in cybersecurity even in an era of fiscal restraint.

Our most important investment is in skilled cyber warriors needed to conduct operations in cyberspace.

Just as DoD developed the world's finest counterterrorism force over the past decade, we need to build and maintain the finest cyber force and operations. We're recruiting, we're training, we're retaining the best and the brightest in order to stay ahead of other nations.

It's no secret that Russia and China have advanced cyber capabilities. Iran has also undertaken a concerted effort to use cyberspace to its advantage.

Moreover, DoD is already in an intense daily struggle against thousands of cyber actors who probe the Defense Department's networks, millions of time a day. Throughout the innovative efforts of our cyber operators, we've been trying to enhance the department's cyber-defense programs.

These systems rely on sensors; they rely on software to hunt down the malicious code before it harms our systems. We actively share our own experience defending our systems with those running the nation's critical private sector networks.

In addition to defending the department's networks, we also help deter attacks. Our cyber adversaries will be far less likely to hit us if they know that we will be able to link to the attack or that their effort will fall against our strong defenses.

The department has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack.
Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment.

Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.

But we won’t succeed in preventing a cyber attack through improved defenses alone. If we detect an imminent threat of attack that will cause significant, physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us to defend this nation when directed by the president.

For these kinds of scenarios, the department has developed that capability to conduct effective operations to counter threats to our national interests in cyberspace.

Let me clear that we will only do so to defend our nation, to defend our interests, to defend our allies and we will only do so in a manner that is consistent with the policy principles and legal frameworks that the department follows for other domains including the law of armed conflict.

Which brings me to the second area of focus, policies and organization. Responding to the cyber threat requires the right policies and organizations across the federal government.

For the past year, the Department of Defense has been working very closely with other agencies to understand where are the lines of responsibility when it comes to cyber defense. Where do we draw those lines? And how do those responsibilities get executed?

As part of that effort, the department is now finalizing the most comprehensive change to our rules of engagement in cyberspace in seven years. The new rules will make clear that the department has a responsibility, not only to defend DoD’s networks, but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace.

These new rules make the department more agile and provide us with the ability to confront major threats quickly.

To execute these responsibilities, we must have strong organization structures in place.

Three years ago, the department took a major step forward by establishing the United States Cyber Command. Under the leadership of General Keith Alexander, a four-star officer who also serves as the director of the National Security Agency.

Cyber Command has matured into what I believe is a world-class organization.

It has the capacity to conduct a full range of missions inside cyberspace. And it’s also working to develop a common, real-time understanding of the threats in cyberspace. The threat picture could be quickly shared with DoD’s geographic and functional combatant commanders, with DHS, with FBI and with other agencies in government. After all, we need to see an attack coming in order to defend against that attack.

And we’re looking at ways to strengthen Cyber Command as well. We must ensure that it has the resources, that it has the authorities, that it has the capabilities required to perform this growing mission. And it must also be able to react quickly to events unfolding in cyberspace and help fully integrate cyber into all of the department’s plans and activities.

And finally, the third area is to build stronger partnerships.

As I’ve made clear, securing cyberspace is not the sole responsibility of the United States military or even the sole responsibility of the United States government. The private sector, government, military, our allies - all share the same global infrastructure and we all share the responsibility to protect it.

Therefore, we are deepening cooperation with our closest allies with the goal of sharing threat information, maximizing shared capabilities and determining malicious activities. The president, the vice president, Secretary of State and I have made cyber a major topic of discussion in nearly all of our bilateral meetings with foreign counterparts.

I recently met with our Chinese military counterparts just a few weeks ago. As I mentioned earlier, China is rapidly growing its cyber capabilities.
In my visit to Beijing, I underscored the need to increase communication and transparency with each other so that we could avoid a misunderstanding or a miscalculation in cyberspace. This is in the interest of the United States, but it’s also in the interest of China.

Ultimately, no one has a greater interest in cybersecurity than the businesses that depend on a safe, secure and resilient global, digital infrastructure.

Particularly those who operate the critical networks that we must help defend. To defend those networks more effectively, we must share information between the government and the private sector about threats in cyberspace.

We’ve made real progress in sharing information with the private sector. But very frankly, we need Congress to act to ensure that this sharing is timely and comprehensive.

Companies should be able to share specific threat information with the government, without the prospect of lawsuits hanging over their head. And a key principle must be to protect the fundamental liberties and privacy in cyberspace that we are all duty bound to uphold.

Information sharing alone is not sufficient. We’ve got to work with the business community to develop baseline standards for our most critical private-sector infrastructure, our power plants, our water treatment facilities, our gas pipelines. This would help ensure that companies take proactive measures to secure themselves against sophisticated threats, but also take common sense steps against basic threats. Although awareness is growing, the reality is that too few companies have invested in even basic cybersecurity.

The fact is that to fully provide the necessary protection in our democracy, cybersecurity legislation must be passed by the Congress. Without it, we are and we will be vulnerable.

Congress must act and it must act now on a comprehensive bill such as the bipartisan Cybersecurity Act of 2012 co-sponsored by Senators Lieberman, Collins, Rockefeller and Feinstein.

(Applause.)

This legislation has bipartisan support, but is victim to legislative and political gridlock like so much else in Washington. That frankly is unacceptable and it should be unacceptable not just to me, but to you and to anyone concerned with safeguarding our national security.

While we wait for Congress to act, the administration is looking to enhance cybersecurity measures under existing authorities, by working with the private sector to promote best practices, increase information sharing.

They are considering issuing an Executive Order as one option to try to deal with the situation, but very frankly there is no substitute for comprehensive legislation and we need to move as far as we can in the meantime. We have no choice because the threat that we face, as I’ve said, is already here.

Congress has a responsibility to act and the President of the United States has constitutional responsibility to defend our country.

I want to urge each of you to add your voice to those who support stronger cyber defenses for our country.

In closing, let me say something that I know the people of New York, along with all Americans, will appreciate.

Before September 11, 2001, the warning signs were there. We weren’t organized. We weren’t ready and we suffered terribly for that lack of attention.

We cannot let that happen again. This is a pre-9/11 moment.

(Applause.)

The attackers are plotting. Our systems will never be impenetrable just like our physical defenses are not perfect, but more can be done to improve them. We need Congress and we need all of you to help in that effort.
I want you to know the Department of Defense is doing our part.

And tonight, I'm asking you to do yours as citizens and as business leaders. Help us innovate. Help us increase the nation's cybersecurity by securing your own networks. Help us remain ahead of the threats that we confront. By doing so, you will help ensure that cyberspace continues to bring prosperity to your companies and to people across the world.

BENS has played an important part in this debate by identifying cybersecurity as a key national security challenge where business and government must partner together.

And so I'd like thank BENS for your leadership in this area and thank you again for your recognition of the efforts that we have made.

But more broadly, let me thank you for your commitment to the dream that guides all of us in this nation.

I talked about my parents as immigrants. And I used to ask my father why did he travel all of that distance to come to a strange land, leaving the comfort of family, it was a poor area in Italy, but why would you leave your comfort of family and travel all that distance to a strange land? And my father said the reason he did it is because he and my mother believed that they could give their children a better life. That is the American dream.

That's what we want for our children. We have achieved that dream because we always have been able to defend our interests and our values. That must remain our most important mission on land, at sea, in the air, in space and yes, in cyberspace. This is not just a responsibility, it is a duty that we owe to our children and their children in the future.

Thank you very much.
Department of Defense Cyberspace Policy Report

A Report to Congress
Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934

November 2011
Contents

INTRODUCTION .................................................................................................................. 1
SECTION I: DESCRIPTION OF POLICY AND LEGAL ISSUES ......................................... 1
SECTION II: DECISIONS OF THE SECRETARY OF DEFENSE ........................................... 10
SECTION III: NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS ........ 10
SECTION IV: CURRENT USE OF CYBER MODELING AND SIMULATION ......................... 10
SECTION V: APPLICATION OF CYBER MODELING AND SIMULATION ......................... 11
ANNEX A: FULL TEXT OF SECTION 934 OF THE NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2011 .......................................................... 11
Introduction

This report is submitted in accordance with the requirements of Section 934 of the Ike Skelton National Defense Authorization Act (NDAA) for Fiscal Year 2011.

Cyberspace is a critical enabler to Department of Defense (DoD) military, intelligence, business and, potentially, civil support operations. While the development and integration of cyber technologies have created many high leverage opportunities for DoD, our increasing reliance upon cyberspace also creates vulnerabilities for both DoD and the Nation.

To more holistically capture these dynamic challenges and opportunities, the Department published the Department of Defense Strategy for Operating in Cyberspace (available at www.defense.gov/news/d20110714cyber.pdf), which identifies five distinct, but interrelated strategic initiatives to support DoD’s cyberspace operations and its national security mission:

- Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential in its military, intelligence, and business operations;
- Employ new defense operating concepts, including active cyber defense, to protect DoD networks and systems;
- Partner closely with other U.S. Government departments and agencies and the private sector to enable a whole-of-government strategy and a nationally integrated approach to cybersecurity;
- Build robust relationships with U.S. Allies and international partners to enable information sharing and strengthen collective cybersecurity; and
- Leverage the Nation’s ingenuity by recruiting and retaining an exceptional cyber workforce and enabling rapid technological innovation.

Section I: Description of Policy and Legal Issues

As described in the Department of Defense Strategy for Operating in Cyberspace, DoD is addressing the complex challenges and opportunities of cyberspace in an integrated manner. DoD is focused on the development and extension of all necessary policies and authorities for its cyberspace operations. As with all of the activities that DoD pursues in the physical world, cyberspace operations are executed with a clear mission and under clear authorities, and they are governed by all applicable domestic and international legal frameworks, including the protection of civil liberties and the law of armed conflict.

The Senate Report (S. Rept. 111-201) accompanying the Senate version of the Ike Skelton NDAA for Fiscal Year 2011 further identified thirteen specific questions on cyber policy for
both DoD and the U.S. Government. This report answers each of the thirteen questions posed in Senate Report 111-201.

1. The development of a declaratory deterrence posture for cyberspace, including the relationship between military operations in cyberspace and kinetic operations. The Committee believes that this deterrence posture needs to consider the current vulnerability of the U.S. economy and government institutions to attack, the relatively lower vulnerability of potential adversaries, and the advantage currently enjoyed by the offense in cyberwarfare.

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. When warranted, we will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we reserve the right to use all necessary means—diplomatic, informational, military, and economic—to defend our Nation, our Allies, our partners, and our interests. In doing so, we will exhaust all options prior to using force whenever we can; we will carefully weigh the costs and risks of action against the costs of inaction; and we will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support wherever possible. For its part, DoD will ensure that the U.S. military continues to have all necessary capabilities in cyberspace to defend the United States and its interests, as it does across all domains.

Deterrence in cyberspace, as with other domains, relies on two principal mechanisms: denying an adversary’s objectives and, if necessary, imposing costs on an adversary for aggression. Accordingly, DoD will continue to strengthen its defenses and support efforts to improve the cybersecurity of our government, critical infrastructure, and Nation. By denying or minimizing the benefit of malicious activity in cyberspace, the United States will discourage adversaries from attacking or exploiting our networks. DoD supports these efforts by enhancing our defenses, increasing our resiliency, and conducting military-to-military bilateral and multilateral discussions.

In addition, the U.S. is working with like-minded nations to establish an environment of expectations, or norms of behavior, that increase understanding of cyber doctrine, and guide Allied policies and international partnerships. At the same time, should the “deny objectives” element of deterrence not prove adequate, DoD maintains, and is further developing, the ability to respond militarily in cyberspace and in other domains. Continuing to improve our ability to attribute attacks is a key to military response options.

Defending the Homeland is an important element of deterrence. DoD will use its significant capability and expertise in support of a whole-of-government approach to protect the Nation. The policy and legal authorities governing DoD’s domestic activities — such as Defense Support to Civil Authorities — extend to cyber operations, as they would in any other domain. DoD will continue to work closely with its interagency partners, including the Departments of Justice and Homeland Security, to address threats to the United States from wherever they originate, through
a whole-of-government approach. The Department is dedicated to the protection of the Nation, and to the privacy and the civil liberties of its citizens.

Deterrence is a whole-of-government proposition. DoD supports the White House Cybersecurity legislative proposal to protect the American people, U.S. critical infrastructure, and our government’s networks and systems more effectively. DoD is working closely with its interagency partners, including the Department of Homeland Security, to increase the cybersecurity of our critical infrastructure. Moreover, DoD continues to work with private sector partners through efforts like the Enduring Security Framework and the Defense Industrial Base Cybersecurity/Information Assurance programs to enhance cybersecurity, reduce vulnerabilities, and encourage the innovation necessary to protect and strengthen the U.S. economy. DoD is working with the Department of State to strengthen ties with our Allies and international partners to enhance mutual security.

2. The necessity of preserving the President’s freedom of action in crises and confrontations involving nations which may pose a manageable conventional threat to the United States but which in theory could pose a serious threat to the U.S. economy, government, or military through cyber attacks.

The Department recognizes that a nation possessing sophisticated and powerful cyber capabilities could attempt to affect the strategic calculus of the United States. In this scenario, an adversary might act in ways antithetical to vital U.S. national interests and attempt to prevent the President from exercising traditional national security options by threatening or implying the launch of a crippling cyber attack against the United States.

Any state attempting such a strategy would be taking a grave risk. DoD recognizes the vital importance of maintaining the President’s freedom of action. The Department is working, with our interagency partners, to ensure no future adversaries are tempted to pursue such a strategy. Our efforts focus on the following three areas:

- First, the Department, in conjunction with the Intelligence Community and Law Enforcement agencies, strives to secure the best possible intelligence about potential adversaries’ cyber capabilities. These efforts are crucial because the United States needs to understand other nations’ cyber capabilities in order to defend against them and to improve our ability to attribute any cyber attacks that may occur. Forensic analysis is a part of attributing attacks, but foreign intelligence collection and international law enforcement cooperation play a key role. In this regard, the co-location of the National Security Agency and United States Cyber Command (USCYBERCOM) provides benefits and efficiencies to the Department for its cyber operations. The National Security Agency’s unique strengths and capabilities provide USCYBERCOM with critical cryptologic support for target and access development, enabling DoD cyberspace operations planning and execution.

- Second, the Department recognizes that strong cyber defenses and resilient information architectures, particularly those connected to critical infrastructure, mitigate the ability of
a future adversary to constrain the President’s freedom of action. If future adversaries are unable to cripple our centers of gravity, they will be more likely to understand that the President has the full menu of national security options available.

- 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 DoD.

3. How deterrence or effective retaliation can be achieved in light of attribution limitations.

The same technical protocols of the Internet that have facilitated the explosive growth of cyberspace also provide some measure of anonymity. Our potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage.

The Department recognizes that deterring malicious actors from conducting cyber attacks is complicated by the difficulty of verifying the location from which an attack was launched and by the need to identify the attacker among a wide variety and high number of potential actors. With this in mind, the Department actively seeks to limit the ability of such potential actors to exploit or attack the United States anonymously in three ways:

- First, the Department seeks to increase our attribution capabilities by supporting innovative research and development in both DoD and the private sector. This research focuses on two primary areas: developing new ways to trace the physical source of an attack, and seeking to assess the identity of the attacker via behavior-based algorithms. In the near future, the Department intends to expand and deploy applications that detect, track, and report malicious activities across all DoD networks and information systems on a near real-time basis. The ability to detect malicious activities quickly allows forensics experts to recover evidence during important windows of opportunity for attribution.

- Second, the Department has significantly improved its cyber forensics capabilities over the past several years. The Intelligence Community and U.S. Cyber Command continue to develop a highly skilled cadre of forensics experts. Additionally, DoD has been the primary supporter of an innovative and effective center of excellence for forensics capabilities at the Defense Cyber Crime Center. This unique organization provides an important nexus of support to both defense and law-enforcement communities, as well as to private sector companies who support DoD.

- Third, in partnership with the Department of Homeland Security, DoD is expanding its international partnerships to increase shared situational awareness, warning capabilities and forensics efforts. The ability to share timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors enables advance
deterrence of malicious activity. Equally important are efforts to work with international partners to bolster cyber forensics capabilities.

4. To the extent that deterrence depends upon demonstrated capabilities or at least declarations about capabilities and retaliatory plans, how and when the Department intends to declassify information about U.S. cyber capabilities and plans or to demonstrate capabilities.

Effective deterrence in cyberspace is founded upon both the security and resilience of U.S. networks and systems, and ensuring that the United States has the capability to respond to hostile acts with a proportional and justified response. The International Strategy for Cyberspace provides a clear statement that the United States reserves the right to use all necessary means—diplomatic, informational, military, and economic—to defend our Nation, our Allies, our partners, and our interests in cyberspace.

The dynamic and sensitive nature of cyberspace operations makes it difficult to declassify specific capabilities. However, the Department has the capability to conduct offensive operations in cyberspace to defend our Nation, Allies and interests. If directed by the President, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict.

5. How to maintain control of or manage escalation in cyberwarfare, through, for example, such measures as refraining from attacking certain targets (such as command and control and critical infrastructure).

The unique characteristics of cyberspace can make the danger of escalation especially acute. For instance, the speed of action and dynamism inherent in cyberspace, challenges of anonymity, and the widespread availability of malicious tools can compound communications and increase opportunities for misinterpretation. As a result, DoD recognizes the clear importance of steps such as the development of transparency and confidence building measures, in addition to further development of international cyberspace norms, to avoid escalation and misperception in cyberspace. DoD and the Department of State are actively engaged with Allies, partners, and other states to build transparency and confidence with traditional adversaries.

The Department also seeks to prevent dangerous escalatory situations by following the same policy principles and legal regimes in its cyberspace operations that govern actions in the physical world, including the law of armed conflict. DoD’s cyberspace operations are subject to careful coordination and review, including the use of cyberspace for intelligence operations. Intelligence, military, and political implications are carefully considered for cyberspace operations as elsewhere.

In collaboration with other U.S. Government agencies, Allies and partners, DoD 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.

Finally, the Department believes that increased transparency minimizes the likelihood that a cyber incident will escalate to a dangerous or unintended level. DoD continues to pursue opportunities for the facilitation and expansion of transparency among key international actors with regard to their command and control, doctrine, and deployment of cyber capabilities. DoD works with international partners to develop confidence building and risk reduction measures to decrease the chance of miscommunication and escalation in cyberspace.

6. The rules of engagement for commanders at various command echelons for responding to threats to operational missions and in normal peacetime operating environments, including for situations in which the immediate sources of an attack are computers based in the United States.

DoD has implemented rules of engagement for the operation and defense of its networks. In current operations that occur in designated Areas of Hostilities, specific rules of engagement have been approved to govern and guide DoD operations in all domains. DoD’s cyber capabilities are integrated into planning and operations under existing policy and legal regimes.

As it continues to build and develop its cyber capabilities and organizational structures, the Department is addressing operational needs by modifying its standing rules of engagement for commanders to enable required decisions and take appropriate actions to defend critical information networks and systems. Due to the interconnectedness and speed that defines cyberspace, these standing rules of engagement will reflect: the implications of cyber threats; the operational demands of DoD’s continuous, worldwide operations; and the need to minimize disruption from collateral effects on networked infrastructure.

DoD recognizes the unique challenge presented by malicious activity coming from within the United States. The Department will support domestic agencies and departments, using its significant capability and expertise in support of a whole-of-government approach to protect the Nation. The policy and legal authorities governing DoD’s domestic activities — such as Defense Support to Civil Authorities — extend to cyber operations, as they would in any other domain. DoD will continue to work closely with its interagency partners, including the Departments of Justice and Homeland Security, to address threats to the United States from wherever they originate, through a whole-of-government approach. The Department is dedicated to the protection of the Nation, and to the privacy and the civil liberties of its citizens.

7. How the administration will evaluate the risks and consequences attendant to penetrations of foreign networks for intelligence gathering in situations where the discovery of the penetration could cause the targeted nation to interpret the penetration as a serious hostile act.

Espionage has a long history and is nearly always practiced in both directions. For the U.S. and many other states, traditional espionage has been a state-sponsored intelligence-gathering function focused on national security, defense, and foreign policy issues. The United States
Government collects foreign intelligence via cyberspace, and does so in compliance with all applicable laws, policies, and procedures. The conduct of all U.S. intelligence operations is governed by long-standing and well-established considerations, to include the possibility those operations could be interpreted as a hostile act.

Classified material pertaining to this section is available in the separate Classified Annex.

8. How DoD shall keep Congress fully informed of significant cyberspace accesses acquired for any purpose that could serve as preparation of the environment for military action.

The Department has been working closely with Congress to improve the reporting schemes for cyberspace operations. DoD will provide quarterly cyber briefings to appropriate Members of Congress and their congressional staff in fulfillment of notification requirements. For sensitive operations that may require out-of-cycle reporting, DoD will ensure that appropriate Members of Congress and their congressional staff receive any necessary additional briefings.

9. The potential benefit of engaging allies in common approaches to cyberspace deterrence, mutual and collective defense, and working to establish norms of acceptable behavior in cyberspace.

The President’s International Strategy for Cyberspace makes clear that hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners, and DoD has been working actively to clarify those expectations within our alliances.

To implement that vision, the Department of Defense Strategy for Operating in Cyberspace emphasizes the importance of building robust relationships with U.S. Allies and partners to strengthen the deterrence of malicious cyberspace activity and to build collective cyber defenses. Through shared warning, capacity building, and joint training activities, international engagement provides opportunities for an exchange of information and new ideas to strengthen U.S. and allied cyber capabilities. DoD continues to coordinate amendments to the National Disclosure Policy that will ensure detailed cyber operations discussions with Allies and international partners.

DoD is actively deepening its engagement on cyber issues with its Allies and international partners. The Department continues to have both senior-level and expert coordinating activities with Australia, Canada, New Zealand, and the United Kingdom. DoD has worked closely with its NATO Allies on cyber issues, including the revised NATO Cyber Policy and associated action plan approved at the June 2011 Ministerial. In further development of our treaty relationships, DoD is strengthening its relationships with Japan and the Republic of Korea. DoD and its Allies and international partners can maximize cyber capabilities, mitigate risk, and deter malicious activities in cyberspace.

The United States is actively engaged in the continuing development of norms of responsible state behavior in cyberspace, making clear that as a matter of U.S. policy, long-standing
international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace's unique aspects may require clarifications in certain areas.

10. The issue of third-party sovereignty to determine what to do when the U.S. military is attacked, or U.S. military operations and forces are at risk in some other respect, by actions taking place on or through computers or other infrastructure located in a neutral third country.

The nature of the DoD response to a hostile act or threat is based upon a multitude of factors, but always adheres to the principles of the law of armed conflict. These responses include taking actions short of the use of force as understood in international law.

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:

- The nature of the malicious cyber activity;
- The role, if any, of the third country;
- The ability and willingness of the third country to respond effectively to the malicious cyber activity; and
- The appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstances.

11. The issue of the legality of transporting cyber "weapons" across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of "overflight rights."

There is currently no international consensus regarding the definition of a "cyber weapon." The often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult. Most of the technology used in this context is inherently dual-use, and even software might be minimally repurposed for malicious action.

The interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains. The law of armed conflict and customary international law, however, provide a strong basis to apply such norms to cyberspace governing responsible state behavior. Significant multinational work remains to clarify the application of norms and principles of customary international law to cyberspace.

As the President recognized in the International Strategy for Cyberspace, the development of norms for state conduct does not require a reinvention of customary international law nor render
existing norms obsolete. Rather, the principled application of existing norms must be developed with our partners and Allies. DoD, in conjunction with other U.S. Government departments and agencies, will continue to work with our partners and Allies to build consensus on the applicability of norms in cyberspace to develop customary international law further.

12. The definition or the parameters of what would constitute an act of war in cyberspace and how the laws of war should be applied to military operations in cyberspace.

The phrase “act of war” is frequently used as shorthand to refer to an act that may permit a state to use force in self-defense, but more appropriately, it refers to an act that may lead to a state of ongoing hostilities or armed conflict. Contemporary international law addresses the concept of “act of war” in terms of a “threat or use of force,” as that phrase is used in the United Nations (UN) Charter. Article 2(4) of the UN Charter 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.” International legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the physical domains (i.e., sea, air, land, and space), also apply to the cyberspace domain.

As in the physical world, a determination of what is a “threat or use of force” in cyberspace must be made in the context in which the activity occurs, and it involves an analysis by the affected states of the effect and purpose of the actions in question.

The particular attributes of cyberspace can make this determination especially difficult, including the detection of the activity, political and/or technical attribution, and a determination if the particular activity is part of a larger military operation, although these are challenges present in the “real world” as well.

Without question, some activities conducted in cyberspace could constitute a use of force, and may as well invoke a state’s inherent right to lawful self-defense. In this context, determining defensive response to even presumptively illegal acts rests with the Commander-in-Chief.


The requirements of the War Powers Resolution apply to “the introduction of United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations.”

Cyber operations might not include the introduction of armed forces personnel into the area of hostilities. Cyber operations may, however, be a component of larger operations that could trigger notification and reporting in accordance with the War Powers Resolution. The Department will continue to assess each of its actions in cyberspace to determine when the requirements of the War Powers Resolution may apply to those actions.
Section II: Decisions of the Secretary of Defense

By approving the *Department of Defense Strategy for Operating in Cyberspace*, the Secretary of Defense has set out comprehensive guidance for the Department's cyberspace activities in defense and support of U.S. national interests. The strategy also provides clear objectives and policies for DoD to take advantage of cyberspace's potential, while recognizing the continued growth of both cyberspace threats and vulnerabilities.

DoD has also worked closely with the Administration to develop its Cybersecurity Legislative Proposal. DoD supports the Administration's efforts to improve cybersecurity for the American people, our critical infrastructure, and the U.S. Government's networks and systems. DoD relies upon U.S. critical civilian infrastructure for its operations. The theft of sensitive information and intellectual capital erodes DoD's effectiveness and the economic vitality upon which our military strength depends.

Section III: National Military Strategy for Cyberspace Operations

The Joint Staff does not intend to modify the National Military Strategy for Cyberspace Operations at this time. To guide the Department's activities in cyberspace, the Secretary of Defense has approved the *Department of Defense Strategy for Operating in Cyberspace*.

Section IV: Current Use of Cyber Modeling and Simulation

Cyber modeling and simulation technologies are rapidly evolving in scope and sophistication. As the size and complexity of networks continue to grow, the need for capabilities to understand and study them has become increasingly apparent. In DoD, the use of these tools and technologies varies greatly depending upon the unique requirements and mission sets of component organizations.

Exploration and refinement of tactics, techniques, and procedures used to defend DoD networks are a key application of modeling and simulation. The use of "test ranges" allows the military to increase awareness, adjust planning, improve resiliency of its networks and systems, and train personnel. DoD's cyber workforce can use these capabilities to increase proficiency through realistic, practical application of techniques and procedures to hone skills for better identification of vulnerabilities and improved remediation response. In addition to new technologies and their application, the use of ranges allows DoD to explore and develop new concepts for its operations in a contained but realistic environment.

The Defense Intelligence Agency (DIA) and several Combatant Commands are developing and using methodologies, analytic techniques, and tools to identify potential cyber vulnerabilities. Modeling and simulation are some of the tools used, but they are still at early stages of development. Including methodologies and modeling in structural analytic techniques provides DoD with a framework to test assumptions and explore the interaction between networks. For instance, the Cyber Operations Research Environment (CORE) provides data necessary to perform predictive strategic analysis on the impact of potential cyber threats. This work
provides the information necessary to prioritize mitigation efforts, increase network security, and preserve the ability of particular systems to perform military missions.

DoD is also pursuing revolutionary approaches to modeling and simulation, such as the National Cyber Range (NCR). The NCR will create a new state-of-the-art capability for large-scale cyber testing. This ability to evaluate cyber technologies, policies, and procedures will be a critical asset to the development of future operations. By enabling testing and analysis under real word conditions, DoD will be able to refine, research, and develop capabilities that can strengthen cyber defenses and revolutionize cybersecurity. The NCR will allow testing of current cyber environments, and it will be the foundation of future modeling and simulation capabilities.

Classified material pertaining to this section is available in the separate Classified Annex.

**Section V: Application of Cyber Modeling and Simulation**

The application of cyber modeling and simulation capabilities can improve current defense and future development activities. These lessons will allow DoD to develop improved architectures and increase the sophistication of its cyber defenses. New capabilities such as the NCR will provide vast improvements in DoD’s ability to model and simulate a variety of networks quickly and at scale. DoD continues to innovate and explore new initiatives that improve our cyberspace strategies and programs.

As cyber technologies and their applications continue to evolve, DoD is exploring the use of modeling and simulation technologies to test and evaluate new cyberspace concepts, policies, and capabilities. These efforts will enable DoD to develop new ideas and adapt to technological trends. Improved modeling and simulation capabilities will further DoD’s efforts to understand and integrate more effectively policy, legal, operational, and technical trends in cyberspace that will allow the Department to identify vulnerabilities, address them, and ensure that the U.S. military continues to have the capability to fulfill its national security mission in defense of the Nation.

Classified material pertaining to this section is available in the separate Classified Annex.

**ANNEX A: FULL TEXT OF SECTION 934 OF THE NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2011**

SEC. 934. REPORT ON THE CYBER WARFARE POLICY OF THE DEPARTMENT OF DEFENSE.

(a) REPORT REQUIRED.—Not later than March 1, 2011, the Secretary of Defense shall submit to Congress a report on the cyber warfare policy of the Department of Defense.

(b) ELEMENTS.—The report required under this section shall include the following:
(1) A description of the policy and legal issues investigated and evaluated by the Department in considering the range H. R. 6523—203 of missions and activities that the Department may choose to conduct in cyberspace.

(2) The decisions of the Secretary with respect to such issues, and the recommendations of the Secretary to the President for decisions on such of those issues as exceed the authority of the Secretary to resolve, together with the rationale and justification of the Secretary for such decisions and recommendations.

(3) A description of the intentions of the Secretary with regard to modifying the National Military Strategy for Cyberspace Operations.

(4) The current use of, and potential applications of, modeling and simulation tools to identify likely cybersecurity vulnerabilities, as well as new protective and remediation means, within the Department.

(5) The application of modeling and simulation technology to develop strategies and programs to deter hostile or malicious activity intended to compromise Department information systems.

(c) FORM.—The report required under this section shall be submitted in unclassified form, but may include a classified annex.
MEMORANDUM OF AGREEMENT
BETWEEN
THE DEPARTMENT OF HOMELAND SECURITY
AND
THE DEPARTMENT OF DEFENSE
REGARDING CYBERSECURITY

1. PARTIES. The parties to this Agreement are the Department of Homeland Security (DHS) and the Department of Defense (DoD).


3. PURPOSE. The purpose of the Agreement is to set forth terms by which DHS and DoD will provide personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the Nation’s cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities. Implementing this Agreement will focus national cybersecurity efforts, increasing the overall capacity and capability of both DHS’s homeland security and DoD’s national security missions, while providing integral protection for privacy, civil rights, and civil liberties.

4. SCOPE. DoD and DHS agree to collaborate to improve the synchronization and mutual support of their respective efforts in support of U.S. cybersecurity. Departmental relationships identified in this Agreement are intended to improve the efficiency and effectiveness of requirements formulation, and requests for products, services, technical assistance, coordination, and performance assessment for cybersecurity missions executed across a variety of DoD and DHS elements. They do not alter existing DoD and DHS authorities, command relationships, or privacy, civil liberties, and other oversight relationships. In establishing a framework to provide mutually beneficial logistical and operational support, this Agreement is not intended to replicate or aggregate unnecessarily the diverse line organizations across technology development, operations, and customer support that collectively execute cybersecurity missions.

5. RESPONSIBILITIES.
A. Department of Homeland Security,
   1) Identify and assign, in coordination with the Department of Defense, a DHS Director, Cybersecurity Coordination who will be in the National Protection and
   CLEARED
   For Open Publication

OCT 13 2010 10
Office of Security Review
Department of Defense

11-S-0123
Programs Directorate and will be located at the National Security Agency (NSA) but will not be in the NSA chain of command. This individual will also act as the DHS Senior Cybersecurity Representative to U.S. Cyber Command (USCYBERCOM).

2) Receive DoD requests for cybersecurity support and consider DoD requirements, as appropriate and consistent with applicable law and DHS mission requirements and authorities, related to operational planning and mission coordination.

3) Identify qualified DHS personnel to perform DHS functions under the sole supervision and direction of DHS officials as follows:
   a. Assign DHS personnel to work at NSA as part of a Joint Coordination Element (JCE) performing the functions of joint operational planning, coordination, synchronization, requirement translation, and other DHS mission support for homeland security for cybersecurity under the direct supervision of the Director, Cybersecurity Coordination;
   b. Assign personnel to work at the NSA Directorate of Acquisition for collaborative acquisition and technology development;
   c. Assign or detail, as appropriate, personnel to work at the National Security Agency/Central Security Services (NSA/CSS) Threat Operations Center (NTOC) to promote joint operational planning, coordination, synchronization, requirement translation, and other DHS mission support for homeland security for cybersecurity; and
   d. Assign representatives from the Office of the General Counsel, Privacy Office, and the Office for Civil Rights and Civil Liberties to support the DHS Director, Cybersecurity Coordination, at NSA, and coordinate with the DoD counterparts identified in paragraph B.2.d.

4) Ensure that DHS personnel have current security clearances (TS/SCI) upon assignment to NSA, including training on the appropriate handling and dissemination of classified and sensitive information in accordance with DoD, Intelligence Community and NSA regulations.

5) Provide funding for DHS mission requirements, salaries, and training unique to DHS personnel for assignments under paragraph 5.A.3.

6) Provide appropriate access, administrative support, and space for an NSA Cryptologic Services Group (CSG) and a USCYBERCOM Cyber Support Element (CSE) collocated with the National Cybersecurity and Communications Integration Center (NCCIC), at DHS, and integration into DHS's cybersecurity operational activities. DHS will provide all necessary DHS equipment and connectivity to permit both CSG and CSE entities the capability to carry out their respective roles and responsibilities.

7) DHS Director, Cybersecurity Coordination.
   a. Provide requests for cybersecurity planning, technology, and where appropriate other support to NSA and USCYBERCOM and advocate for such requests based on DHS requirements to protect Federal Executive branch, non-DoD, non-national security systems, and U.S. critical infrastructure and key resources.
   b. Convey to and coordinate within DHS any NSA and USCYBERCOM requests for support or requirements regarding cybersecurity operations.
c. Participate in and lead, as appropriate, joint planning and other processes.
d. Promote and facilitate strong communications between DHS and DoD senior leadership, including that of NSA, on cybersecurity matters of joint interest, including engaging in joint operational planning and mission coordination.
e. Maintain cognizance of DHS and, as appropriate, of DoD, NSA, and USCYBERCOM cybersecurity activities, to assist in deconfliction and promote synchronization of those activities.
f. Assist in coordinating DoD and DHS efforts to improve cybersecurity threat information sharing between the public and private sectors to aid in preventing, detecting, mitigating, and/or recovering from the effects of an attack, interference, compromise, or incapacitation related to homeland security and national security activities in cyberspace.

B. Department of Defense.

1) Direct the Director of NSA (DIRNSA) and Commander, USCYBERCOM, to undertake collaborative activities and provide cybersecurity support envisioned in this agreement and subsequent implementing agreements.

2) National Security Agency.

a. Assign an NSA SES-equivalent to serve as the NSA lead to the Joint Coordination Element (JCE). This NSA official will coordinate and work with the DHS Director, Cybersecurity Coordination in carrying out the activities of the Joint Coordination Element. This NSA official will not be in the DHS chain of command, and his or her performance ratings will be prepared by NSA with input from the DHS Director, Cybersecurity Coordination. This NSA official will supervise and direct all NSA personnel assigned to the JCE.

b. Receive and coordinate DHS requests for cybersecurity support and consider DHS requirements, as appropriate and consistent with applicable law and NSA mission requirements and authorities, in operational planning and mission coordination.

c. Provide appropriate access, facilities, and administrative support (including necessary equipment and connectivity) to support the Director, Cybersecurity Coordination and DHS personnel assigned or detailed to the three entities listed below. NSA will provide all necessary NSA equipment and connectivity to permit DHS personnel with the capability to carry out their roles and responsibilities.
   i. NSA Directorate of Acquisition
   ii. Joint Coordination Element to be located at NSA
   iii. NSA/CSS Threat Operations Center

d. Identify representatives from its Office of the General Counsel and Privacy Office to work with counterparts at DoD, USCYBERCOM, and DHS to support the implementation of this Agreement.

e. Collocate a Cryptologic Services Group at the NCCIC at DHS, for support to and operational synchronization with DHS's cybersecurity operations and the National Cyber Incident Response Plan (NCIRP).

f. Assign or detail qualified personnel in accordance with this Agreement both to serve in JCE positions and in CSG positions as mutually agreed.
g. Engage with DHS and USCYBERCOM in joint operational planning and mission coordination.

h. Provide funding for NSA mission requirements, salaries and training unique to NSA for personnel identified in B.2.c.

3) USCYBERCOM.
   a. Receive DHS requests for cybersecurity support and consider DHS requirements, as appropriate and consistent with applicable law and USCYBERCOM mission requirements and authorities, in operational planning and mission coordination.
   b. Collocate a Cyber Support Element at the NCCIC at DHS, for support to and operational synchronization with DHS's cybersecurity operations and the NCIRP.
   c. Assign qualified personnel to CSE positions.
   d. As needed to implement this Agreement, provide, on a reimbursable basis, appropriate access, administrative support and space for DHS personnel.
   e. Provide funding for USCYBERCOM mission requirements and training unique to its personnel during the assignment.
   f. Engage with DHS and NSA in joint operational planning and mission coordination.

C. Joint DoD-DHS.
   1) Synchronize the roles and relationships of the proposed DoD Integrated Cyber Center (ICC) and the current DHS National Cybersecurity and Communications Integration Center (NCCIC).
   2) Develop agenda of appropriate supporting actions, including consideration of the establishment of a Joint Program Office (JPO).
   3) Develop jointly appropriate agreements, including necessary funding mechanisms, to implement the objectives and responsibilities of this Agreement pursuant to applicable authority.

6. OVERSIGHT. To oversee the activities described in the preceding paragraphs, the Deputy Secretary of Homeland Security and the Deputy Secretary of Defense will conduct monthly oversight meetings supported by the DHS Deputy Under Secretary, National Protection and Programs Directorate (NPPD); the Principal Deputy Under Secretary of Defense for Policy and the Director of NSA/Commander, USCYBERCOM.

7. POINTS OF CONTACT.

Philip Reitinger  James N. Miller
Deputy Under Secretary  Principal Deputy Under Secretary
National Protection and  of Defense for Policy
Programs Directorate  Department of Defense
Department of Homeland Security  2100 Defense Pentagon
Washington, DC 20528  Washington, DC 20301-2100
(703) 235-  (703) 697- 
8. OTHER PROVISIONS. Nothing in this Agreement is intended to conflict with law, regulation, Presidential order or directive, or the directives of DHS or DoD. If a term of this Agreement is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this Agreement shall remain in full force and effect. This Agreement shall be interpreted and implemented in a manner that respects and complies with (and does not abrogate) the statutory and regulatory responsibilities of the Secretary of Homeland Security and the Secretary of Defense. This Agreement does not obligate funds.

9. EFFECTIVE DATE. This Agreement is effective upon signature of both parties.

10. MODIFICATION AND REVIEW. This Agreement may be modified upon the mutual written consent of the parties. This Agreement will be reviewed by the parties after one year.

11. TERMINATION. The terms of this Agreement, as modified with the consent of both parties, will remain in effect until terminated. Either party upon 30 days written notice to the other party may terminate this Agreement.

APPROVED BY:

Janet Napolitano
Secretary of Homeland Security

Date: 1-31-10

Robert Gates
Secretary of Defense

Date: 9-24-10
MEMORANDUM OF AGREEMENT
BETWEEN THE
SECRETARY OF DEFENSE
AND THE
DIRECTOR OF NATIONAL INTELLIGENCE

The Defense Intelligence Components provide a full range of intelligence products and analysis to a broad spectrum of consumers from military forces in the field to senior policy makers across the federal government. These efforts are intertwined with the national intelligence efforts overseen by the Director of National Intelligence.

In recognition of the crucial importance of coordinated intelligence efforts to the national security of the United States and pursuant to 10 U.S.C. § 113, 10 U.S.C. § 137, the National Security Act of 1947, as amended, and the Intelligence Reform and Terrorism Prevention Act of 2004, the Secretary of Defense and the Director of National Intelligence agree to the following:

1. The official serving in the position of Under Secretary of Defense for Intelligence shall be dual-hatted as the Director of Defense Intelligence within the Office of the Director of National Intelligence. As the Under Secretary of Defense for Intelligence, this official shall report to the Secretary and Deputy Secretary of Defense. As the Director of Defense Intelligence, this official shall report to the Director of National Intelligence.

2. As the Under Secretary of Defense for Intelligence, this official shall retain the responsibilities and exercise the authorities as assigned by the Secretary of Defense.

3. As the Director of Defense Intelligence, this official shall report directly to the DNI and serve as the principal advisor to the Director of National Intelligence regarding Defense Intelligence matters. The Director of Defense Intelligence shall have responsibilities as determined by the Director of National Intelligence in consultation with the Secretary of Defense and promulgated separately.

4. Nothing in this memorandum shall be construed to alter the statutory responsibilities or authorities of either the Secretary of Defense or the Director of National Intelligence.
This Agreement takes effect on the date of the last signature below and remains in effect unless terminated by either Party with 30 days advanced written notice to the other Party or by mutual written agreement of the Parties. This Agreement may be modified at any time by mutual written agreement of the Parties. The Parties will review this Agreement every two years to determine whether it should continue or be terminated by mutual written agreement.

SIGNED:

J. Michael McConnell  
Director of National Intelligence  
Date: 21 MAY 07

Robert M. Gates  
Secretary of Defense  
Date: 5-17-07

230
International Law in Cyberspace

Remarks
Harold Hongju Koh
Legal Advisor U.S. Department of State
USCYBERCOM Inter-Agency Legal Conference
Ft. Meade, MD
September 18, 2012

As prepared for delivery

Thank you, Colonel Brown, for your kind invitation to speak here today at this very important conference on "the roles of cyber in national defense." I have been an international lawyer for more than thirty years, a government lawyer practicing international law for more than a decade, and the State Department's Legal Adviser, for nearly 3 ½ years. While my daily workload covers many of the bread and butter issues of international law—diplomatic immunity, the law of the sea, international humanitarian law, treaty interpretation—like many of you, I find more and more of my time is spent grappling with the question of how international law applies in cyberspace.

Everyone here knows that cyberspace presents new opportunities and new challenges for the United States in every foreign policy realm, including national defense. But for international lawyers, it also presents cutting-edge issues of international law, which go to a very fundamental question: how do we apply old laws of war to new cyber-circumstances, staying faithful to enduring principles, while accounting for changing times and technologies?

Many, many international lawyers here in the U.S. Government and around the world have struggled with this question, so today I'd like to present an overview of how we in the U.S. Government have gone about meeting this challenge. At the outset, let me highlight that the entire endeavor of applying established international law to cyberspace is part of a broader international conversation. We are not alone in thinking about these questions; we are actively engaged with the rest of the international community, both bilaterally and multilaterally, on the subject of applying international law in cyberspace.

With your permission, I'd like to offer a series of questions and answers that illuminate where we are right now— in a place where we've made remarkable headway in a relatively short period of time, but are still finding new questions for each and every one we answer. In fact, the U.S. Government has been regularly sharing these thoughts with our international partners. Most of the points that follow we have not just agreed upon internally, but made diplomatically, in our submissions to the UN Group of Governmental Experts (GGE) that deals with information technology issues.

I. International Law in Cyberspace: What We Know

So let me start with the most fundamental questions:

Question 1: Do established principles of international law apply to cyberspace?

Answer 1: Yes, international law principles do apply in cyberspace. Everyone here knows how cyberspace opens up a host of novel and extremely difficult legal issues. But on this key question, this answer has been apparent, at least as far as the U.S. Government has been concerned. Significantly, this view has not necessarily been universal in the international community. At least one country has questioned whether existing bodies of international law apply to the cutting edge issues presented by the Internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace. But the United States has made clear our view that established principles of international law do apply in cyberspace.

Question 2: Is cyberspace a law-free zone, where anything goes?

Answer 2: Emphatically no. Cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraint.

Think of it this way. This is not the first time that technology has changed and that international law has been asked to deal with those changes. In particular, because the tools of conflict are constantly evolving, one relevant body of law — international humanitarian law, or the law of armed conflict — alternatively anticipates technological innovation, and contemplates that its existing rules will apply to such innovation. To be sure, new technologies raise new issues and thus, new questions. Many of us in this room have struggled with such questions, and we will continue to do so over many years. But to those who say that established law is not up to the task, we must articulate and build consensus around how it applies and reassess from there whether and what additional understandings are needed. Developing common understandings about how these rules apply in the context of cyberactivities in armed conflict will promote stability in this area.

That consensus-building work brings me to some questions and answers we have offered to our international partners to explain how both the law of going to war (jus ad bellum) and the laws that apply in conducting war (jus in bello) apply to cyberactivity:

Question 3: Do cyber activities ever constitute a use of force?
Answer 5: Yes. Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law. In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes. Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.

Question 4: May a State ever respond to a computer network attack by exercising a right of national self-defense?

Answer 4: Yes. A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof. As the United States affirmed in its 2011 National Strategy for Cyberspace, "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."

Question 5: What rules apply to computer network attacks?

Answer 5: Yes, in the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools. The principles of necessity and proportionality limit uses of force in self-defense and would regulate what may constitute a lawful response under the circumstances. There is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.

Question 6: Must attacks distinguish between military and nonmilitary objectives?

Answer 6: Yes. The jus in bello principle of distinction applies to computer network attacks undertaken in the context of an armed conflict. The principle of distinction applies to cyber activities that amount to an "attack" — as that term is understood in the law of war — in the context of an armed conflict. As in any form of armed conflict, the principle of distinction requires that the intended effect of the attack must be to harm a legitimate military target. We must distinguish military objectives—that is, objects that make an effective contribution to military action and whose destruction would offer a military advantage — from civilian objects, which under international law are generally protected from attack.

Question 7: Does the law respect the principle of proportionality?

Answer 7: Yes. The jus in bello principle of proportionality applies to computer network attacks undertaken in the context of an armed conflict. The principle of proportionality prohibits attacks that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated. Parties to an armed conflict must assess what the expected harm to civilians is likely to be, and weigh the risk of such collateral damage against the importance of the expected military advantage to be gained. In the cyber context, this rule requires parties to a conflict to assess: (1) the effects of cyber weapons on both military and civilian infrastructure and users, including shared physical infrastructure (such as a dam or a power grid) that would affect civilians; (2) the potential physical damage that a cyber attack may cause, such as death or injury that may result from effects on critical infrastructure; and (3) the potential effects of a cyber attack on civilian objects that are not military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are military objectives.

Question 8: How should States assess their cyber weapons?

Answer 8: States should undertake a legal review of weapons, including those that employ a cyber capability. Such a review should entail an analysis, for example, of whether a particular capability would be inherently indiscriminate, i.e., that it could not be used consistent with the principles of distinction and proportionality. The U.S. Government undertakes at least two stages of legal review of the use of weapons in the context of armed conflict — first, on an evaluation of new weapons to determine whether their use would be permissible under the laws of war; and second, specific operations employing weapons are always reviewed to ensure that each particular operation is also compliant with the law of war.

Question 9: In this analysis, what role does State sovereignty play?

Answer 9: States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict. The physical infrastructure that supports the internet and the computer activities is generally located in sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered.

Question 10: Are States responsible when cyber acts are undertaken through proxies?

Answer 10: Yes. States are legally responsible for activities undertaken through "proxy actors," who act on the State's instructions or under its direction or control. The ability to mask one's identity and geography in cyberspace and the resulting difficulties of timely, high-confidence attribution can create significant challenges for States in identifying, investigating, and accurately responding to threats. But putting attribution problems aside for a moment, established international law does address the question of proxy actors. States are legally responsible for activities undertaken through relatively private actors, who act on the State's instructions or under its direction or control. If a State exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State itself had committed it. These rules are designed to
ensure that States cannot hide behind putatively private actors to engage in conduct that is internationally wrongful.

II. International Law in Cyberspace: Challenges and Uncertainties

These ten answers should give you a sense of how far we have come in doing what any good international lawyer does: applying established law to new facts, and explaining our positions to other interested lawyers. At the same time, there are obviously many more issues where the questions remain under discussion. Let me identify three particularly difficult questions that I don't intend to answer here today. Instead, my hope is to shed some light on some of the cutting-edge legal issues that we'll all be facing together over the next few years:

Unresolved Question 1: How can a use of force regime take into account all of the novel kinds of effects that States can produce through the click of a button?

As I said above, the United States has affirmed that established jus ad bellum rules do apply to uses of force in cyberspace. I have also noted some clear-cut cases where the physical effects of a hostile cyber activity would be comparable to what a kinetic action could achieve: for example, a bomb might break a dam and flood a civilian population, but insertion of a line of malicious code from a distant computer might just as easily achieve that same result. As you all know, however, there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by "force." At the same time, the difficulty of reaching a definitive legal conclusion or consensus among States on when and under what circumstances a hostile cyber action would constitute an armed attack does not automatically suggest that we need an entirely new legal framework specific to cyberspace. Outside of the cyber-context, such ambiguities and differences of view have long existed among States.

To cite just one example of this, the United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response — such responses must still be necessary and of course proportionate. We recognize, on the other hand, that some other countries and commentators have drawn a distinction between the "use of force" and an "armed attack," and view "armed attack" — triggering the right to self-defense — as a subset of uses of force, which passes a higher threshold of gravity. Part of the point here is not to rehash old debates, but to illustrate that States have long had to sort through complicated jus ad bellum questions. In this respect, the existence of complicated cyber questions relating to jus ad bellum is not in itself a new development; it is just applying old questions to the latest developments in technology.

Unresolved Question 2: What do we do about "dual-use infrastructure" in cyberspace?

As you all know, information and communications infrastructure is often shared between State militaries and private, civilian communities. The law of war requires that civilian infrastructure not be used to seek to immunize military objectives from attack. But when, exactly, are the jus in bello rules to be implemented in cyberspace? Parties to an armed conflict will need to assess the potential effects of a cyber attack on computers that are not military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are valid military objectives. Parties will also need to consider the harm to the civilian uses of such infrastructure in performing the necessary proportionality review. Any number of factual scenarios could arise, however, which will require a careful, fact-intensive legal analysis in each situation.

Unresolved Question 3: How do we address the problem of attribution in cyberspace?

As I mentioned earlier, cyberspace significantly increases an actor's ability to engage in attacks with "plausible deniability," by acting through proxies. I noted that legal tools exist to ensure that States are held accountable for those acts. What I want to highlight here is that many of these challenges — in particular, those concerning attribution — are as much questions of a technical and policy nature rather than exclusively or even predominantly questions of law. Cyberspace remains a new and dynamic operating environment, and we cannot expect that all answers to the new and confounding questions we face will be legal ones.

Those questions about effects, dual-use, and attribution are difficult legal and policy questions that existed long before the development of cyber tools, and that will continue to be a topic of discussion among our allies and partners as cyber tools develop. Of course, there remain many other difficult and important questions about the application of international law to activities in cyberspace — for example, about the implications of sovereignty and neutrality law, enforcement mechanisms, and the obligations of States concerning "hacktivists" operating from within their territory. While these are not questions that I can address in this brief speech, they are critically important questions on which international lawyers will focus intensely in the years to come.

And just as cyberspace presents challenging new issues for lawyers, it presents challenging new technical and policy issues. Not all of the issues I've mentioned are susceptible to clear legal answers derived from existing precedents — in many cases, quite the contrary. Answering these tough questions within the framework of existing law, consistent with our values and accounting for the legitimate needs of national security, will require a constant dialogue between lawyers, operators, and policymakers. All that we as lawyers can do is to apply in the cyber context the same rigorous approach to these hard questions that arise in the future, as we apply every day to what might be considered more traditional forms of conflict.

III. The Role of International Law in a "Smart Power" Approach to Cyberspace

This, in a nutshell, is where we are with regard to cyberconflict: We have begun work to build consensus on a number of answers, but questions continue to arise that must be answered in the months and years ahead. Beyond these questions and answers and unresolved questions, though, lies a much bigger picture, one that we are very focused on at the State Department. Which brings me to my final two questions:

Final Question 1: Is international humanitarian law the only body of international law that applies in cyberspace?

Final Answer 1: No. As important as international humanitarian law is, it is not the only international law that applies in cyberspace.
Obviously, cyberspace has become pervasive in our lives, not just in the national defense arena, but also through social media, publishing and broadcasting, expressions of human rights, and expansion of international commerce, both through online markets and online commercial techniques. Many other bodies of international and national law address these activities, and how these different bodies of law overlap and interact with the laws of cyber conflict is something we will all have to work out over time.

Take human rights. At the same time that cyber activity can pose a threat, we all understand that cyber-communication is increasingly becoming a dominant mode of expression in the 21st century. More and more people express their views not by speaking on a soap box at Speakers’ Corner, but by blogging, tweeting, commenting, or posting videos and commentaries. The 1948 Universal Declaration of Human Rights (UDHR) – adopted more than 70 years ago – was remarkably forward-looking in anticipating these trends. It says: “everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” (emphasis added) In short, all human beings are entitled to certain rights, whether they choose to exercise them in a city square or an internet chat room. This principle is an important part of our global diplomacy, and is encapsulated in the Internet Freedom agenda about which my boss, Secretary Clinton, has spoken so passionately.

You all know of this Administration’s efforts not just in the areas of cyber conflict, but also in many other cyber areas: cybersecurity, cybercommerce, fighting child pornography and other forms of cybercrime, stopping intellectual property piracy, as well as promoting free expression and human rights. So the cyber conflict issues with which this group grapples do not constitute the whole of our approach to cyberspace; they are an important part – but only a part of this Administration’s broader “smart power” approach to cyberspace.

What I have outlined today are a series of answers to cyberspace questions that the United States is on the record as supporting. I have also suggested a few of the challenging questions that remain before us, and developments over the next decade will surely produce new questions. But you should not think of these questions and answers as just a box to check before deciding whether a particular proposed operation is lawful or not. Rather, these questions and answers are part of a much broader foreign policy agenda, which transpires in a broader framework of respect for international law.

That leads to my final question for this group: Why should U.S. Government lawyers care about international law in cyberspace at all?

The answer: Because compliance with international law frees us to do more, and do more legitimately, in cyberspace, in a way that more fully promotes our national interests. Compliance with international law in cyberspace is part and parcel of our broader “smart power” approach to International law as part of U.S. foreign policy.

It is worth noting two fundamentally different philosophies about International law. One way to think about law, whether domestic or international, is as a straitjacket, a pure constraint. This approach posits that nations have serious, legitimate interests, and legal regimes restrict their ability to carry them out. One consequence of this view is that, since law is just something that constrains, it should be resisted whenever possible. Resisting so-called “extensions” of the law to new areas often seems attractive; because, after all, the old laws weren’t built for these new challenges anyway, some say, so we should tackle those challenges without the legal straitjacket, while leaving the old laws behind.

But that is not the United States Government’s view of the law, domestic or international. We see law not as a straitjacket, but as one great university calls it when it confers its diplomas, a body of “wise restraints that make us free.” International law is not purely constraint, it frees us and empowers us to do things we could never do without law’s legitimacy. If we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we do take will earn enhanced legitimacy worldwide for their adherence to the rule of law.

Those are not new themes, but I raise them here because of how they resonate squarely with the strategy we have been pursuing in cyberspace over the past few years. Of course, the United States has impressive cyber-capabilities; it should be clear from the bulk of my discussions that adherence to established principles of law does not prevent us from using those capabilities to achieve important ends. But we also know that we will be safer, the more that we can rally other States to the view that these established principles do impose meaningful constraints, and that there is already an existing set of laws that protect our security in cyberspace. And the more widespread the understanding that cyberspace follows established rules – and that we live by them – the stronger we can be in pushing back against those who would seek to introduce brand new rules that may be contrary to our interests.

That is why, in our diplomacy, we do not whisper about these issues. We talk openly and bilaterally with other countries about the application of established international law to cyberspace. We talk about these issues multilaterally, at the UN Group of Governmental Experts and at other fora, in promoting this vision of compliance with international law in cyberspace. We talk about them regionally, as when we recently co-sponsored an ASEAN Regional Forum event to focus the international community’s attention on the problems of proxy actors engaging in unlawful conduct in cyberspace. Preventing proxy attacks on us is an important interest, and as part of our discussions we have outlined the ways that existing international law addresses this problem.

The diplomacy I have described is not limited to the legal issues this group of lawyers is used to facing in the operational context. These issues are interconnected with countless other cyber issues that we face daily in our foreign policy, such as cybersecurity, cyber-commerce, human rights in cyberspace, and public diplomacy through cybertools. In all of these areas, let me repeat again, compliance with international law in cyberspace is part and parcel of our broader smart power approach to International law as part of U.S. foreign policy – and thinking actively together about how best to promote that compliance – can only free us to do more, and to do more legitimately, in the emerging frontiers of cyberspace, in a way that more fully promotes our U.S. national interests.

Thank you very much.
DEPARTMENT OF DEFENSE STRATEGY
FOR OPERATING IN CYBERSPACE

JULY 2011
INTRODUCTION

STRATEGIC CONTEXT

FIVE STRATEGIC INITIATIVES

Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential

Strategic Initiative 2: Employ new defense operating concepts to protect DoD networks and systems

Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy

Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity

Strategic Initiative 5: Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation

CONCLUSION
"Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."

- 2010 National Security Strategy

Cyberspace is a defining feature of modern life. Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people. As Internet usage continues to expand, cyberspace will become increasingly woven into the fabric of everyday life across the globe.

U.S. and international businesses trade goods and services in cyberspace, moving assets across the globe in seconds. In addition to facilitating trade in other sectors, cyberspace is itself a key sector of the global economy. Cyberspace has become an incubator for new forms of entrepreneurship, advances in technology, the spread of free speech, and new social networks that drive our economy and reflect our principles. The security and effective operation of U.S. critical infrastructure — including energy, banking and finance, transportation, communication, and the Defense Industrial Base — rely on cyberspace, industrial control systems, and information technology that may be vulnerable to disruption or exploitation.

Along with the rest of the U.S. government, the Department of Defense (DoD) depends on cyberspace to function. It is difficult to overstate this reliance; DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations.

The Department and the nation have vulnerabilities in cyberspace. Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity — the security of the technologies that we use each day. Moreover, the continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its mission. Today, many foreign nations are working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD’s information infrastructure. Moreover, non-state actors increasingly threaten to penetrate and disrupt DoD networks and systems. We recognize that there may be malicious activities on DoD networks and systems that we have not yet detected.

DoD, working with its interagency and international partners, seeks to mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy and civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S. prosperity and security. How the Department leverages the opportunities of cyberspace, while managing inherent uncertainties and reducing vulnerabilities, will significantly impact U.S. defensive readiness and national security for years to come.
STRATEGIC CONTEXT

“There is no exaggerating our dependence on DoD’s information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field.”

- 2010 Quadrennial Defense Review

DoD’s Strengths and Opportunities in Cyberspace

As does the nation as a whole, DoD relies on a secure and reliable cyberspace that protects fundamental freedoms, privacy, and the free flow of information. In support of both U.S. core commitments and national security, DoD has significant strengths and opportunities in cyberspace. The U.S. military’s ability to use cyberspace for rapid communication and information sharing in support of operations is a critical enabler of DoD missions. More broadly, DoD’s depth of knowledge in the global information and communications technology sector, including its cybersecurity expertise, provides the Department with strategic advantages in cyberspace.

The quality of the United States’ human capital and knowledge base in both the public and private sectors provides DoD with a strong foundation on which to build current and future cyber capabilities. DoD has played a crucial role in building and leveraging the technological prowess of the U.S. private sector through investments in people, research, and technology. DoD will continue to embrace this spirit of entrepreneurship and work in partnership with these communities and institutions to succeed in its future cyberspace activities.

Given the dynamism of cyberspace, nations must work together to defend their common interests and promote security. DoD’s relationship with U.S. allies and international partners provides a strong foundation upon which to further U.S. international cyberspace cooperation. Continued international engagement, collective self-defense, and the establishment of international cyberspace norms will also serve to strengthen cyberspace for the benefit of all.

Cyber Threats

“The very technologies that empower us to lead and create also empower those who would disrupt and destroy.”

- 2010 National Security Strategy

The Internet was designed to be collaborative, rapidly expandable, and easily adaptable to technological innovation. Information flow took precedence over content integrity; identity authentication was less important than connectivity. The Internet’s original designers could not have imagined the extent of its vital and growing role for DoD and its operations. The global scope of DoD networks and systems presents adversaries with broad opportunities for exploitation and attack.
Low barriers to entry for malicious cyber activity, including the widespread availability of hacking tools, mean that an individual or small group of determined cyber actors can potentially cause significant damage to both DoD and U.S. national and economic security. Small-scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to U.S. national security.

In developing its strategy for operating in cyberspace, DoD is focused on a number of central aspects of the cyber threat; these include external threat actors, insider threats, supply chain vulnerabilities, and threats to DoD’s operational ability. DoD must address vulnerabilities and the concerted efforts of both state and non-state actors to gain unauthorized access to its networks and systems.

Foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from U.S. networks and those of U.S. allies and industry partners. Moreover, this threat continues to evolve as evidence grows of adversaries focusing on the development of increasingly sophisticated and potentially dangerous capabilities.

The potential for small groups to have an asymmetric impact in cyberspace creates very real incentives for malicious activity. Beyond formal governmental activities, cyber criminals can control botnets with millions of infected hosts. The tools and techniques developed by cyber criminals are increasing in sophistication at an incredible rate, and many of these capabilities can be purchased cheaply on the Internet. Whether the goal is monetary, access to intellectual property, or the disruption of critical DoD systems, the rapidly evolving threat landscape presents a complex and vital challenge for national and economic security.

Some cyber threats also may come from insiders. Malicious insiders may exploit their access at the behest of foreign governments, terrorist groups, criminal elements, unscrupulous associates, or on their own initiative. Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DoD, and national security, can be devastating.

Software and hardware are at risk of malicious tampering even before they are integrated into an operational system. The majority of information technology products used in the United States are manufactured and assembled overseas. The reliance of DoD on foreign manufacturing and development creates challenges in managing risk at points of design, manufacture, service, distribution, and disposal.

Potential U.S. adversaries may seek to exploit, disrupt, deny, and degrade the networks and systems that DoD depends on for its operations. DoD is particularly concerned with three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems.
Cyber threats to U.S. national security go well beyond military targets and affect all aspects of society. Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks and systems that control critical civilian infrastructure. Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption. DoD operations—both at home and abroad—are dependent on this critical infrastructure.

While the threat to intellectual property is often less visible than the threat to critical infrastructure, it may be the most pervasive cyber threat today. Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. As military strength ultimately depends on economic vitality, sustained intellectual property losses erode both U.S. military effectiveness and national competitiveness in the global economy.
Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential.

"Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."

- 2010 Quadrennial Defense Review

Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD’s national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests. Furthermore, these efforts must include the performance of essential missions in a degraded cyber environment.

As directed by the National Security Strategy, DoD must ensure that it has the necessary capabilities to operate effectively in all domains—air, land, maritime, space, and cyberspace. At all levels, DoD will organize, train, and equip for the complex challenges and vast opportunities of cyberspace. To this end, the Secretary of Defense has assigned cyberspace mission responsibilities to United States Strategic Command (USSTRATCOM), the other Combatant Commands, and the Military Departments. Given its need to ensure the ability to operate effectively in cyberspace and efficiently organize its resources, DoD established U.S. Cyber Command (USCYBERCOM) as a sub-unified command of USSTRATCOM. The establishment of USCYBERCOM reflects DoD’s need to:

- Manage cyberspace risk through efforts such as increased training, information assurance, greater situational awareness, and creating secure and resilient network environments;

- Assure integrity and availability by engaging in smart partnerships, building collective self defenses, and maintaining a common operating picture; and

- Ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most.

USSTRATCOM has delegated to USCYBERCOM the responsibility for synchronizing and coordinating Service components within each branch of the military, including U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. 10th Fleet, the 24th Air Force, U.S. Marine Corps Forces Cyber Command, and U.S. Coast Guard Cyber Command. A key organizational concept behind the stand-up of USCYBERCOM is its co-location with the National Security Agency (NSA). Additionally, the Director of the National Security Agency is dual-hatted as the Commander of USCYBERCOM. Co-location and dual-hatting of these separate and distinct
organizations allow DoD, and the U.S. government, to maximize talent and capabilities, leverage respective authorities, and operate more effectively to achieve DoD’s mission.

Because degraded cyberspace operations for extended periods may be a reality and disruption may occur in the midst of a mission, DoD will fully integrate a complete spectrum of cyberspace scenarios into exercises and training to prepare U.S. Armed Forces for a wide variety of contingencies. A cornerstone of this activity will be the inclusion of cyber red teams throughout war games and exercises. Operating with a presumption of breach will require DoD to be agile and resilient, focusing its efforts on mission assurance and the preservation of critical operating capability.

These efforts will be supported by the development of increasingly resilient networks and systems. In the case of a contingency involving network failure or significant compromise, DoD must be able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another. Multiple networks can add diversity, resiliency, and mission assurance to cyberspace operations. DoD is investing in research to identify options for shifting its operations to secure networks at scale and across the full spectrum of operations.

**Strategic Initiative 2: DoD will employ new defense operating concepts to protect DoD networks and systems.**

"Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient."

- 2010 National Security Strategy

The implementation of constantly evolving defense operating concepts is required to achieve DoD’s cyberspace mission today and in the future. As a first step, DoD is enhancing its cyber hygiene best practices to improve its cybersecurity. Second, to deter and mitigate insider threats, DoD will strengthen its workforce communications, workforce accountability, internal monitoring, and information management capabilities. Third, DoD will employ an active cyber defense capability to prevent intrusions onto DoD networks and systems. Fourth, DoD is developing new defense operating concepts and computing architectures. All of these components combine to form an adaptive and dynamic defense of DoD networks and systems.
Most vulnerabilities of and malicious acts against DoD systems can be addressed through good cyber hygiene. Cyber hygiene must be practiced by everyone at all times; it is just as important for individuals to be focused on protecting themselves as it is to keep security software and operating systems up to date. DoD will integrate the private sector’s continuous renewal method to harden its own computing devices and sustain its cyber hygiene best practices. Further, good cyber hygiene extends to the maintenance of information security, the promotion of good cybersecurity practices for users and administrators alike, secure network design and implementation, and the employment of smart and effective network and configuration management. This holistic effort will provide protection, monitoring, maintenance, design, and care for DoD networks and systems to assure their security and integrity.

People are the Department’s first line of defense in sustaining good cyber hygiene and reducing insider threats. To mitigate the insider threat and prevent dangerous disclosures of sensitive and classified information from occurring, DoD will strengthen and go beyond the current information assurance paradigm, including the exploration of new operating concepts to reduce vulnerabilities. DoD’s efforts will focus on communication, personnel training, and new technologies and processes. DoD seeks to foster a stronger culture of information assurance within its workforce to assure individual responsibility and deter malicious insiders by shaping behaviors and attitudes through the imposition of higher costs for malicious activity. This cultural shift will be enabled by new policies, new methods of personnel training, and innovative workforce communications.

As malicious cyber activity continues to grow, DoD has employed active cyber defense to prevent intrusions and defeat adversary activities on DoD networks and systems. Active cyber defense is DoD’s synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks.

To foster resiliency and smart diversity in its networks and systems, DoD will explore new and innovative approaches and paradigms for both existing and emerging challenges. These efforts will include development and integration in the areas of mobile media and secure cloud computing. DoD will continue to be adaptive in its cyberspace efforts, embracing both evolutionary and rapid change.
Strategic Initiative 3: DoD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.

"Neither government nor the private sector nor individual citizens can meet this challenge alone—we will expand the ways we work together."

- 2010 National Security Strategy

The challenges of cyberspace cross sectors, industries, and U.S. government departments and agencies; they extend across national boundaries and through multiple components of the global economy. Many of DoD’s critical functions and operations rely on commercial assets, including Internet Service Providers (ISPs) and global supply chains, over which DoD has no direct authority to mitigate risk effectively. Therefore, DoD will work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to share ideas, develop new capabilities, and support collective efforts to meet the crosscutting challenges of cyberspace.

In order to enable a whole-of-government approach, DoD will continue to work closely with its interagency partners on new and innovative ways to increase national cybersecurity. An example of one critical initiative is the 2010 memorandum of agreement signed by the Secretary of Defense and Secretary of Homeland Security to align and enhance cybersecurity collaboration. An enhanced partnership between DHS and DoD will improve national cybersecurity in three important ways. First, the formalized structure reaffirms the limits that current law and policy set on DoD and DHS collaboration. Second, joint participation in program planning will increase each department’s mission effectiveness; specifically, it will improve a shared understanding of cybersecurity needs and ensure the protection of privacy and civil liberties. Third, the arrangement will conserve limited budgetary resources. This agreement will help DHS to best protect the Executive Branch .gov domain, work in partnership with state, local, and tribal governments, partner with the private sector, and coordinate the defense of U.S. critical infrastructure.

DoD is also partnering with the Defense Industrial Base (DIB) to increase the protection of sensitive information. The DIB comprises the public and private organizations and corporations that support DoD through the provision of defense technologies, weapons systems, policy and strategy development, and personnel. To increase protection of DIB networks, DoD launched the Defense Industrial Base Cyber Security and Information Assurance (CS/IA) program in 2007. Building upon this program, DoD is also establishing a pilot public-private sector partnership intended to demonstrate the feasibility and benefits of voluntarily opting into increased sharing of information about malicious or unauthorized cyber activity and protective cybersecurity measures.

Given the rapid pace of change that characterizes cyberspace, DoD will continue to work with interagency partners and the private sector to examine new collaborative approaches to cybersecurity. These efforts will include DoD’s support of DHS in leading interagency efforts to identify and mitigate cyber vulnerabilities in the nation’s critical infrastructure. Success will require additional pilot programs, business models, and policy frameworks to foster public-
private synergy. Public-private partnerships will necessarily require a balance between regulation and volunteerism, and they will be built on innovation, openness, and trust. In some cases, incentives or other measures will be necessary to promote private sector participation. DoD’s efforts must also extend beyond large corporations to small and medium-sized businesses to ensure participation and leverage innovation. A collaborative national effort will develop common and workable solutions to policy problems that both increase cybersecurity and further the public good.

DoD will continue to support the development of whole-of-government approaches for managing risks associated with the globalization of the information and communications technology sector. Many U.S. technology firms outsource software and hardware factors of production, and in some cases, their knowledge base, to firms overseas. Additionally, increases in the number of counterfeit products and components demand procedures to both reduce risk and increase quality. Dependence on technology from untrusted sources diminishes the predictability and assurance that DoD requires, and DoD will work with DHS and its interagency partners to better identify and address these risks. The global technology supply chain affects mission critical aspects of the DoD enterprise, along with core U.S. government and private sector functions, and its risks must be mitigated through strategic public-private sector cooperation.

Strategic Initiative 4: DoD will build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.

"Through its foreign defense relationships, the United States not only helps to deter crises but also improves its effectiveness in responding to them."

- 2010 Quadrennial Defense Review

In support of the U.S. International Strategy for Cyberspace and in collaboration with its interagency partners, DoD will seek increasingly robust international relationships to reflect our core commitments and common interests in cyberspace. The development of international shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence. By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense. Cyberspace is a network of networks that includes thousands of ISPs across the globe; no single state or organization can maintain effective cyber defenses on its own.

DoD’s international engagement will support the U.S. International Strategy for Cyberspace and the President’s commitment to fundamental freedoms, privacy, and the free
flow of information. DoD will assist U.S. efforts to advance the development and promotion of international cyberspace norms and principles that promote openness, interoperability, security, and reliability. The Department will work with interagency and international partners to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserve the right to defend these vital national assets as necessary and appropriate. These efforts will sustain a cyberspace that provides opportunities to innovate and yield benefits for all.

As international cyberspace cooperation continues to develop, DoD will advance its close cyberspace cooperation with its allies to defend U.S. and allied interests in cyberspace. DoD will work closely with its allies and international partners to develop shared warning capabilities, engage in capacity building, and conduct joint training activities. Engagement will create opportunities to initiate dialogues for sharing best practices in areas such as forensics, capability development, exercise participation, and public-private partnerships. Further, the development of burden sharing arrangements can play to each nation’s core strengths and capabilities; this will bolster areas where partners are less proficient, increase capacity, and strengthen collective cybersecurity.

DoD will expand its formal and informal cyber cooperation to a wider pool of allied and partner militaries to develop collective self-defense and increase collective deterrence. DoD will create new opportunities for like-minded states to work cooperatively based on shared principles; expanded and strengthened relationships with allies and international partners can maximize scarce cyber capabilities, mitigate risk, and create coalitions to deter malicious activities in cyberspace. These coalitions will serve to augment DoD’s formal alliances and partnerships and increase broader cybersecurity.

**Strategic Initiative 5: DoD will leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation.**

"We will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet these challenges.

—2010 National Security Strategy"

The defense of U.S. national security interests in cyberspace depends on the talent and ingenuity of the American people. DoD will catalyze U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace and achieve DoD objectives. Technological innovation is at the forefront of national security, and DoD will foster rapid innovation and enhance its acquisition processes to ensure effective cyberspace operations. DoD will invest in its people, technology, and research and development to create and sustain the cyberspace capabilities that are vital to national security.

The development and retention of an exceptional cyber workforce is central to DoD’s strategic success in cyberspace and each of the strategic initiatives outlined in this strategy. DoD will assess its cyber workforce, requirements, and capabilities on a regular basis. The development of the cyber workforce is of paramount importance to DoD.
The demand for new cyber personnel is high, commensurate with the severity of cyber threats. DoD must make itself competitive if it is to attract technically skilled personnel to join government service for the long-term. To achieve its objectives, DoD will focus on the establishment of dynamic programs to attract talent early, and the Department will leverage the 2010 Presidential Initiative to improve federal recruitment and hiring processes. DoD will also work with the Executive Office of the President to explore strategies designed to streamline hiring practices for its cyber workforce and exchange programs to allow for "no penalty" cross-flow of cyber professionals between the public and private sectors to retain and grow innovative cyber talent.

Beyond these recruiting, education, and training initiatives, adoption and scaling of cross-generational mentoring programs will allow DoD to grow a gifted cyber talent base for future defense and national security missions. Paradigm-shifting approaches such as the development of Reserve and National Guard cyber capabilities can build greater capacity, expertise, and flexibility across DoD, federal, state, and private sector activities. Opportunities for exchanges and continuing education programs will be explored by DoD, infusing an entrepreneurial approach in cyber workforce development. Continued education and training will be hallmarks of the cyber workforce, preserving, and developing DoD's intellectual capital.

To replicate the dynamism of the private sector and harness the power of emerging computing concepts, DoD’s acquisition processes for information technology will adopt five principles. First, speed is a critical priority. DoD’s acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years. Second, DoD will employ incremental development and testing rather than a single deployment of large, complex systems. Third, DoD will be willing to sacrifice or defer some customization to achieve speedier incremental improvements. Fourth, DoD’s information technology needs—from modernizing nuclear command and control systems to updating word-processing software—will adopt differing levels of oversight based on the Department’s prioritization of critical systems. Fifth, improved security measures will be taken with all of the systems that DoD buys, including software and hardware. No backdoor can be left open to infiltration; no test module can be left active. These principles will be a part of, and reinforced by, DoD’s trusted defense systems and supply chain risk mitigation strategies. For its hardware, software, architecture, systems, and processes, DoD will take a security in depth approach to design, acquisition, and implementation of trustworthy systems.

DoD will also promote opportunities for small and medium-sized businesses, and the Department will work with entrepreneurs in Silicon Valley and other U.S. technology innovation hubs to move concepts rapidly from innovative idea, to pilot program, to scaled adoption across the DoD enterprise. DoD’s cyberspace acquisition programs will reflect the adaptive nature of cyberspace; it will emphasize agility, embrace new operating concepts, and foster collaboration across the scientific community and the U.S. government as a whole.
DoD will explore game changing approaches, including new architectures, to strengthen DoD’s defense capabilities and make DoD systems more resistant to malicious activity. DoD will pursue revolutionary technologies that rethink the technological foundations of cyberspace. To do so, DoD will partner with leading scientific institutions to develop new, safe, and secure cyberspace capabilities that are significantly more resistant to malicious activity.

The development of the National Cyber Range will enable the success of these and other efforts, allowing DoD, other U.S. government entities, and potentially non-U.S. government partners to test and evaluate new cyberspace concepts, policies, and technologies. Although the U.S. military routinely exercises units on target ranges and in a variety of simulations, DoD has had limited capability to simulate cyberspace operations. The National Cyber Range, which allows the rapid creation of numerous models of networks, is intended to enable the military and others to address this need by simulating and testing new technologies and capabilities.

To encourage private sector participation in the development of robust cyberspace capabilities, DoD will empower organizations to serve as clearing houses for innovative concepts and technologies, rewarding firms that develop impactful and innovative technologies. Beyond its engagement with established centers of technological excellence, DoD will leverage the innovation and agility of small businesses and entrepreneurs through initiatives such as Small Business Innovation Research (SBIR), creative joint ventures, and targeted investments and grants in emerging and untested concepts.

The nation’s people, technology, and dynamism provide DoD with a strong foundation on which to build its military and civilian workforce and advance its technological capabilities. DoD will continue to develop robust cyberspace capabilities, and the Department will support interagency efforts to actively engage public and private institutions to encourage cybersecurity innovation. DoD will invest in future personnel and capabilities to achieve its cyberspace objectives and support U.S. national security.
CONCLUSION

“A failure by the Department to secure its systems in cyberspace would pose a fundamental risk to our ability to accomplish defense missions today and in the future.”
- 2010 Quadrennial Defense Review

National security is being redefined by cyberspace. In addition to opportunities, DoD faces significant cyberspace challenges. The Department’s military, intelligence, and business operations all depend upon cyberspace for mission success. The Department of Defense Strategy for Operating in Cyberspace assesses these challenges and opportunities and sets a strategic approach for DoD’s cyber mission.

The Department’s five strategic initiatives offer a roadmap for DoD to operate effectively in cyberspace, defend national interests, and achieve national security objectives. Each initiative is distinct, yet necessarily connected with the other four. Across the strategy, activities undertaken in one initiative will contribute to DoD’s strategic thinking and lead to new approaches in the others.

By pursuing the activities in this strategy, DoD will capitalize on the opportunities afforded to the Department by cyberspace; defend DoD networks and systems against intrusions and malicious activity; support efforts to strengthen cybersecurity for interagency, international, and critical industry partners; and develop robust cyberspace capabilities and partnerships. This strategy will guide the Department’s defense of U.S. interests in cyberspace so that the United States and its allies and partners may continue to benefit from the innovations of the information age.
Panel III:

Emerging Technologies

Moderator: Viet Dinh
The Impact of Technology on National Security Law

Angeline Chen and Clark Walton

Our technological powers increase, but the side effects and potential hazards also escalate.

—Alvin Toffler

If you think technology can solve your technology problems, then you don't understand the problems and you don't understand the technology.

—Bruce Schneier

In this chapter, we take on the daunting task of tracking the technological advances over the past five decades that have most impacted US national security law. The objective—challenging at any point in history given mankind's hallmark of pursuing innovation throughout the ages—is now nigh impossible due to a simple truism: technology has always—and will always—outstrip the law. As coined by Intel's co-founder, Gordon E. Moore, nearly fifty years ago in 1965, Moore's law of constant exponential expansion of technology is alive and well.1 Given the breadth and depth of the issue thus, inevitably, we will fail to some degree, either by overlooking coverage of or linkage to a key technology with indisputable impact, or by failing to apply a more thorough analysis with respect to the interdependencies of some other technological advance's influence on the laws that underpin the national security of our country. That said, we attempt to identify key themes in this area that have permeated history in the national security law domain and will continue to do so in the future.

The impact of technology and emergent advances on national security cannot be denied.2 More critically, the very nature of this impact today is different from in the past, particularly within the context of the law. The advances in past centuries that gave birth historically to technology-fueled "revolutions" relied equally upon not just invention, but accessibility. It was not the sophistication
or brilliance of technological innovation that led to the Industrial or Information Revolutions, but what people—in particular, the common man—actually used, often in a manner or for purposes different from the original intent.3

Today, like the elusive butterfly flapping its wings, daily technological innovations, and perhaps even more so, usage innovations, how people utilize technologies and capabilities that are now easily accessible to the general populace, are continually changing the conditions for the critical social infrastructure that supports the global community. As computers have moved out of large university basements and, for example, into our back pockets and purses, information that would have taken days or weeks to deliver to remote areas now travels literally at the speed of light, through series of fiber optic cables and satellites worldwide, to its intended destination. Conversely, sensitive information that governments, state and non-state actors, and individuals desired to either protect or obtain, became imminently more vulnerable and accessible by virtue of both the means and methods by which it is gathered, stored, distributed, and managed.

Following is a small sampling of technological advances that have radically changed society and global commerce over the past fifty years or so, indicating how emergent and/or evolving technologies have impacted our world:

- 1950s: Boeing introduces the first commercial jet airliner in 1958; domestic service soon connects New York and Los Angeles. The laser beam is created, leading to today's wide range of uses from whitening teeth to tracking missiles. The integrated circuit is introduced in 1959.

- 1960s: Black and Decker introduces cordless tools in 1961 and a NASA contract extends this concept to space for use by astronauts. The first programmable industrial robot is installed on a GM assembly line in New Jersey. The first communications satellite is launched in 1962, enabling global live broadcasting and connectivity via satellite worldwide. A consultant for General Electric develops the light-emitting diode (LED), a groundbreaking technology that allows computers to convey information simply and cheaply. Programmers at the Massachusetts Institute of Technology develop the video game SpaceWar, introducing the concept of mass digital role-playing and simulation. 1964 sees the first unmanned aerial vehicles and during the Vietnam War, 1000 remotely piloted AQM-34 Ryan Firebees are deployed. The 1960s closed with the creation of ARPANET in 1969.
50TH ANNIVERSARY

- 1970s: This decade ushered in fiber optics, cell phones, electronic ignition, and magnetic resonance imaging. In 1978, the Global Positioning System is developed, although the technology is not made available to the general public until 2000 when President Clinton allows access to non-military users. Genetic engineering is born, eventually producing vaccines, clones, insulin, disease prevention techniques, and a new branch of ethics. Personal computers become widely available in the mid-1970s.

- 1980s: This decade sees the advent of the microchip.

- 1990s: Lithium rechargeable batteries and DVDs hit the market in 1991 and 1995, respectively. Thanks to Pioneer, recordable DVDs are available by 1997. Debit cards are launched by Visa in 1995. The 1990s likewise saw a continual advance in cheaper digital storage capabilities and options. In 1991, the Persian Gulf War is recognized as the first major conflict where "modern" technology (including advanced "smart" bombs and precision-guided navigational and targeting capabilities) played a visibly substantial role.

- 2000s: In 2002, IEEE publishes a wireless network standard—IEEE 802.16—that facilitates wireless communications up to a 30-mile radius at speeds that are comparable to DSL and cable broadband. 2002 also saw the introduction of a lifelike 3-d virtual online environment, Second Life, invented by Linden Labs. Social media sites such as Facebook and Twitter, cloud computing, radio-frequency identification (RFID) technology, and nanotechnology continue to have reverberating effects on societal infrastructures while carrying national security implications. Post-September 2001 and various international armed conflicts including those in Afghanistan, Iraq, and elsewhere, see increased usage of technology in the battlefield including, but not limited to, drones, robots, surveillance and other technologies designed for or converted to military use.

Examination of any of the above-referenced technologies alone and their influence in the national security domain could warrant an in-depth and lengthy analysis. To give adequate treatment here to the impact that technology has had on any facet of American society in the last fifty years, let alone the complex issues of national security law, would be impossible.

What constitutes a reasonable expectation of privacy under the Fourth Amendment of the U.S. Constitution when 47 percent of all adults, and 59 percent of all Internet users, use at least one social networking web site such as Facebook, LinkedIn, or Twitter, and they post their likes and dislikes, pictures
of friends, geographic location at points in time, and other personal information on literally a daily basis.24

Or, in the military context, can a cyber event directed by one nation-state and aimed at another constitute an act of war worthy of a kinetic response, and, even if so, how can you be certain exactly who is attacking you?

The works we have selected and referenced herein are intended to give the reader a flavor for the ways in which the American legal system has struggled to adapt to an almost daily changing landscape of novel technical issues that challenge long-held traditional notions of Constitutional and international law. As illustrated by the examples above, in today’s hyper-connected society, analogies to decades old legal precedent sometimes proves cumbersome and at times feel like trying to shove square pegs into round holes. Governments, courts, legal scholars, and legislators alike continue to struggle with these issues, and undoubtedly will continue to do so for many more decades to come.

I. Compilations and Books about Technology and National Security Law

All around us are the consequences of the most significant technological, and hence cultural, revolution in generations.

—Lawrence Lessig

Luckily, America still has a number of smart, thoughtful lawyers, policy makers, and strategists, many of whom have vision and foresight to apply their formidable critical thinking skills to the rapidly changing landscape. In the past decade alone, numerous symposia and conferences have been held wherein subject matter experts have discussed, written, and debated the continuing convergence (and sometimes conflicts or contradictions) of emergent technology and national security law. Listed herein are collections of papers from a number of these symposia and conferences, which have added to the considerable volume of research in this area:

Symposium papers: Law at the intersection of national security, privacy, and technology, 88 Tex. L. Rev. 1 (June 2010).

Available at: https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=4+J.+Nat%27s+Security+L.+%26+Pol%27s+y+%2c+13+%26+src=smi&srcid=3B15&key=918430a94428da509ec07470217717 ***
Symposium: The Fourth Amendment at the International Border, 78 Miss. L. J. 1 (Winter 2008).


ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

II. Technology-related Criminal Law and Intelligence Law

For better or worse, that is true with any new innovation, certainly any
new technological innovation. There's many good things that come out of it,
but also some bad things. All you can do is try to maximize the good stuff
and minimize the bad stuff.

—Steve Case

From the advance of new technologies from the telephone to the iPhone, as
their use becomes commonplace in society, courts and legal scholars alike must
come to grips with the impact those technologies may have on national security
and accompanying privacy law and policy issues. The following are a sampling
of both scholars' analyses of the legal implications of various technological in-
novations of the 20th century, and a non-exclusive listing of seminal federal
court cases that have influenced and continue to influence national security
law and policy.

A. Articles

Gil, L., "Bad intent or just a bad day? Fourth amendment implica-
tions raised by technological advances in security screening." 16 B.U.
J. Sci. & Tech. L. 231 (Summer 2010). Available at: http://www
.bu.edu/law/central/jd/organizations/journals/scitech/volume162
/documents/Gil_WEB.pdf

Dahl, J.Y. and A.R., Saetnan. "It all happened so slowly"—On control-
ling function creep in forensic DNA databases. Int'l Journal of Law,
at: http://brage.bibsys.no/politith/bitstream/URN:NBN:no-
bibsys_brage_16984/5/it%20all%20happened%20%20slowly.pdf

Kerr, O.S., "The Fourth Amendment and new technologies: Con-
stitutional myths and the case for caution,” 102 Mich. L. Rev. 801
.cfm?abstract_id=421560

Covey, R.D., "Pervasive surveillance and the future of the Fourth
Amendment,” 80 Miss. L. J. 1289 (Summer 2011). Available at:

Penney, S., "National security surveillance in an Age of Terror: Statutory
powers & charter limits," 48 Osgood Hall L.J. 247 (Summer 2010).


Yang, D.W. et al., "Countering the cyber-crime threat," 43 Am. Crim. L. Rev. 201 (2006). Available at: https://litigation-essentials.lexisnexis.com/webcd/app/action=DocumentDisplay&crawId=1&srcType=smi&srcId=3B15&doctype=cite&docId=43+Am.+Crim.+L.+Rev.+201&key=cd3c67d0ae998585fd3b72368b6f784***


B. Case law


121
ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

Katz v. United States, 389 US 347 (1967). The concurrence by Justice Harlan set forth the constitutional test for a reasonable expectation of privacy. The case involved taping a microphone to a public telephone booth. Justice Stewart's majority opinion made clear that the opinion spoke to criminal cases, not national security cases. Justice White's concurrence more directly states that criminal warrant procedures should not apply if surveillance is duly authorized by the Executive Branch for national security reasons. Available at: http://supreme.justia.com/cases/federal/us/389/347/case.html

United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn., 2001). Held that provisions of the Computer Fraud and Abuse Act, 18 U.S.C. §1030 et seq., applies to conduct originating outside the United States. In this case, a Russian hacker was convicted of conduct originating in Russia that caused harm within the United States (he hacked a commercial computer system and then demanded $10,000 to be hired as a security consultant for the company or he would delete critical system data). (Note the USA PATRIOT Act expanded the definition of “protected computer” in the CEA to include computers outside the U.S., so long as they had an impact on interstate/foreign commerce or communications of the U.S.). Available at: http://securitylaw.info/pdfs/175_F_Supp_2d_367.pdf

United States v. Jones, 565 U.S. _____ (slip opinion, 2012). Held law enforcement must comply with the 4th Amendment/obtain warrants to put GPS trackers on cars for extended periods of time. Opinion re-visits the Katz framework/may show how the U.S. Supreme Court will view/analyze new technologies as they apply to Fourth Amendment protections going forward. Available at: https://www.eff.org/sites/default/files/filenode/scorussjones.pdf

In re Application of the United States, 809 F. Supp. 2d 113 (E.D.N.Y. 2011). Gives treatment to a request by the federal government for privately held cell phone location data. Significant because it is one of several cases finding that probable cause is required for the government to obtain access such data under certain circumstances, not the lower “specific and articulable facts” standard contained in the Stored Communications Act. Available at: https://www.eff.org/sites/default/files/MDCSLOpinion.pdf
C. Legislation

The Computer Fraud and Abuse Act, 18 U.S.C. §1030 et seq. Notably, see 18 U.S.C. §1030(a)(1) as it specifically criminalizes hacking to access/obtain national security information that could be used to injure the United States or aid a foreign power. Although as of the writing of this document, this provision still has yet to be charged in practice. Available at: http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf


The Foreign Intelligence Surveillance Act, 50 U.S.C § 1801 et seq. Available at: http://www.law.cornell.edu/uscode/text/50/chapter-36

III. Technology and Espionage Law

Otherwise, we will not be able to defeat the U.S. imperialists who boast of their technological superiority.

—Kim Il-sung

As the public enjoys the novelty and convenience of new and innovative technologies, government entities work to both (1) use emerging technologies to their advantage to collect and analyze intelligence on potential threats to national security, and (2) understand and use publicly available technologies for both intelligence and counterintelligence purposes, all the while mindful in each case of a Constitution whose framers could not have possibly contemplated the complex legal and policy questions presented by today’s technological advances. A collection of scholarly articles, cases, and key United States law dealing with certain of these issues follows.

A. Articles

ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY


Stoll, Cliff. *Stalking the Wily Hacker* (May 1988 Vol. 31. No. 5 COMMUNICATION OF THE ACM). The article documents Stoll's tracking of a foreign cyber intruder in the University of California's computer systems in the mid-late 1980's (and his interactions with US military and federal agencies while doing so), which in 1990 led to the prosecution and conviction of hacker Markus Hess in Germany for espionage on behalf of the KGB. Available at: http://pdf.textfiles.com/academics/wilyhacker.pdf

B. CASE LAW


*United States v. Squillacote*, 221 F.3d 542 (4th Cir. 2000). An interesting read and Foreign Intelligence Surveillance Act (FISA) ruling. Defendants were agents of a foreign power (East Germany and later the Russians (SVRR)) convicted of espionage. The federal FISA court allowed 550 consecutive days of wiretapping/surveillance of defendants and also dealt with the minimization requirements for such an extended period of surveillance. Available at: http://bulk.resource.org/courts.gov/c/F3/221/221.F3d.542.-98-61.99-4089.99-4088.html

124
United States v. Scarfo, 180 F. Supp. 2d 572 (D. N.J. 2001)—This case involved the use of a "key stroke logger" and the Classified Information Procedures Act. A criminal case, but CIPA seems to be more espionage related as it prevents the disclosure of classified materials to criminal defendants and by extension the public. The FBI used a keystroke logger, the details of which were classified Secret, to obtain the defendant’s password and decrypt incriminating information. The case walks through the review process of CIPA and ultimately denies disclosure of classified details to the defendant. Available at: http://scholar.google.com/scholar_case?case=12151354094043657712&q=United+States+v.+Scarfo&hl=en&as_sdt=2002

C. Legislation

The Foreign Intelligence Surveillance Act, 50 U.S.C § 1801 et seq. Available at: http://www.law.cornell.edu/uscode/text/50/chapter-36
Classified Information Procedures Act, 18 U.S.C. App. III §1 et seq. Available at: http://www.law.cornell.edu/uscode/html/uscode18a/usc_sup_05_18_10_sq3.html

IV. Technology-Related Information Security and Economic Security Laws

One of the tests of leadership is the ability to recognize a problem before it becomes an emergency.

—Arnold Glasgow

Even a paranoid can have enemies.

—Henry Kissinger

The laws relating to information security and economic security have likewise advanced over the past fifty years with respect to attempts to address evolving technologies facilitating these areas critical to our national security. From unauthorized access to malicious manipulation to outright theft, the threats to both sensitive and proprietary information (such as trade secrets, intellectual property and confidential data relating to sensitive technologies, and our financial systems) that serve as the backbone for our technological, societal, and economic edge are increasing continually. The importance of being proactive in this area cannot be over-emphasized. The United States, whether discussing federal government or U.S. industry, has historically been a frontrunner
in spending on research and development. And yet, no amount of investment can see positive returns if the resulting inventions are stolen through cyber intrusions. Nor can the most sensitive technologies be harnessed as a component of the government's national security framework if it sold to the highest bidder without regard to the impact of the technology's disclosure to our country's national security posture. Similarly, given the global nature of the world's economy and increasing sophistication of overseas investors, governmental attempts to constrain the free market arena of mergers and acquisitions can pose significant challenges for regulators.

The references cited in this section attempt to identify analyses and legal authorities relating to the securing of sensitive technical data and information as well as protective restrictions imposed upon business activities and information driven by economic concerns arising from the disclosure or unauthorized access to technology or information deemed to be directly relevant to national security. As seen in some of the case law in this section as well as the section above addressing Criminal and Intelligence Law, the convergence of these areas has in some instances led to direct constitutional challenges under the First, Fourth, and Fifth Amendments, at times with results that might surprise some.

A. Articles


Gravell, W., Some observations along the road to 'national information power,' 9 Duke L. Comp. and Int'l L. 401 (Spring 1999). Available at: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1235&context=djcl


Ciluffo, F.J., "Bad guys and good stuff: when and where will the cyber threats converge?" 12 DePaul Bus. L.J. 131 (Fall/Spring 1999/2000). Available at: https://litigation-essentials.lexisnexis.com/webcd/app/action=DocumentDisplay&crawlid=1&doctype=cite&docid=12+DePaul+Bus.+L.J.+131&srctype=smi&srcid=3B15&key=c1f31339fda4c6b567195e6268a6c8 ***


B. Case Law

In re Grand Jury Subpoena to Boucher, 2007 WL 4246473 (D. Vt. Nov. 29, 2007). The defendant's password was considered testimonial in nature, and therefore was deemed privileged. On appeal, the grand jury modified the original request and rather than having the defendant produce his password, instead required him to provide an unencrypted version of the information on the defendant's computer (leading to the district court's denial of the defendant's motion to quash). Available at: http://www.crowell.com/PDF/Inre-Boucher.pdf


U.S. v. Ficoco, No. 10-CR-00509 (D. Colo. Jan 23, 2012). The judge in this case compelled the defendant to produce her password in order to allow access to data encrypted upon her laptop. Many
believe the ruling directly undermines Fifth Amendment protections. Available at: https://www.eff.org/cases/us-v-fricosu

Department of State Notice: Termination of ineligible status and statutory debarment pursuant to Section 38(g)(4) of the AECA and Section 127.7 of the ITAR for ITT Corporation, Fed. Reg. Vol. 75, No. 34 p. 7650 (Monday, February 22, 2010). In 2007, ITT received one of the largest penalties ever levied ($100M) in a criminal case for illegally exporting night vision equipment to the People's Republic of China in violation of the ITAR. ITT's Night Vision division was concurrently debarred and prohibited from participating directly or indirectly in exports of defense articles and defense services while ITT was required to enter into a consent agreement with the US State Department which detailed penalties and mandated remedial compliance measures that the corporation had to satisfy before it would be considered for reinstatement following a minimum period of one year's debarment. Available at: https://www.federalregister.gov/articles/2010/02/22/2010-3413/termination-of-ineligible-status-and-statutory-debarment-pursuant-to-section-38g4-of-the-arms-export

C. Legislation


ABA STANDING COMMITTEE ON LAW AND NATIONAL SECURITY


USA PATRIOT Act of 2001. Section 105 of the PATRIOT Act authorizes the development of a national network of electronic crime task forces, for the purpose of addressing electronic crimes including potential attacks against critical infrastructure and financial payment systems. Section 816 of the Act authorizes the establishment of computer forensic laboratories focused on forensic work relating to seized or intercepted computer evidence related to criminal activity. Available at: http://epic.org/privacy/terrorism/hr3162.html/

V. Technology, the Law of Armed Conflict and International Law

_We live in an age that is driven by information. Technological breakthroughs... are changing the face of war and how we prepare for war._

—William J. Perry

Finally, in our last section, we acknowledge the impact of emerging technology in the context of armed conflict and international law. Learned scholars have engaged in lively debates regarding whether the use of new weapons systems (e.g., unmanned drones) is compatible with international law, particularly when combined with a sometimes changing landscape of what constitutes war or armed conflict under _jus cogens_ or even general principles of international law. Moreover, the ongoing and relentless discourse regarding the nature (and existence) of cyber warfare will undoubtedly continue as governments, scholars, and others struggle with the interpretation and applicability of laws that attempt to wrestle and force electrons into the same jurisprudence that took
decades to develop following far more traditional acts of armed aggression and acts of war.

The blurring demarcation, sometimes complete removal, of the territorial borders that define sovereignty in the cyber environment complicates the analysis. So does the inextricable integration of U.S. government assets with private sector assets that constitute our critical infrastructure. An estimated 98% of U.S. government communications travel over private sector owned and operated networks.

A. ARTICLES


SOTH ANNIVERSARY


Richardson, J.C., "Struxnet as cyberwarfare: Applying the law of war to the virtual battlefield" (July 22, 2011). Available at SSRN: http://ssrn.com/abstract=1892888

VI. Conclusion

Any sufficiently advanced technology is indistinguishable from magic.
—Arthur C. Clarke

The best way to predict the future is to invent it.
—Alan Kay

Clarke's memorable quote, issued in 1973 by the famous science fiction writer (who notably also sketched out the model for geosynchronous satellite orbits) captures succinctly how many view emergent technology, viz., with amazement and enthusiasm (sometimes with dread and skepticism) but nevertheless without much interest in understanding the inner workings or probing much further beyond what the technology can demonstrably accomplish. And yet, as skeptics of magic will proceed to determine how the trick is done, in the real and very serious domain of national security, in today's volatile global theater, America must seek to find a way to provide and uphold the codified guidance that will ensure that our country's national security objectives are sufficiently and legally met. We must accomplish this even as the very landscape in which those laws are being employed around the world is changing.

With increasing speed, these "magical" advanced technologies will continuously extend and expand the capabilities of the governments and individuals who have access to them—both domestic and overseas—beyond any existing penumbra of applicable or analogous law. As these emergent technologies re-craft the fabric of the societies from which our existing laws arose, lawyers and drafters of laws—particularly those in the national security field—must rise to a new challenge: that of integrating innovation and imagination with the shaping and practice of those laws that will establish and sustain the rule of law and adapt to the evolving environments in which they must be applied. To accomplish this, we must collectively imagine and anticipate the furthest reaches of what mankind can invent and achieve technologically, and strive to shape and apply the laws that would govern us accordingly.
Hacking tool kits, available free online, fuel growing cyberspace arms race

By Robert O'Harrow Jr., Published: November 13

Ryan Linn’s hacks into corporate networks have become almost a matter of routine. On one recent morning, he woke up at his home near the Research Triangle in eastern North Carolina and walked down to an extra bedroom that he uses as an office. He sat at a workbench laden with computers, signed on to one of them and loaded a program called Metasploit. Sipping a Diet Coke, Linn typed out a few commands and casually launched an attack on a network thousands of miles away. A few seconds later, a report came back: The network had been penetrated. How would he like to proceed? Chalk up another one for Metasploit, an automated tool kit that makes breaking into networks almost as easy for experienced hackers as ordering food off an online menu.

Metasploit and a host of similar tools are becoming as commonplace for many hackers as Firefox and Microsoft Office are for regular computer users.

They are part of an escalating arms race in cyberspace, where millions of attacks and intrusions occur every day. By prepackaging the myriad computer commands that penetrate and exploit target networks, hackers have dramatically eased the process.

Security researchers and consultants, including Linn, use such hacking tools to identify vulnerabilities and help organizations patch them. Bad-guy hackers, known as black hats, and cyberwarriors use similar illicit kits to spy on, steal from and wreak havoc in corporate and government computers.
Metasploit and many other hacker tool kits are available free to anyone who has an Internet connection.

Linn acknowledges the irony. But he likened Metasploit and other tool kits to a “Swiss army knife” and said the positive features “far outweigh the negatives.”

“Metasploit is a tool designed for researchers and security professionals, but just like many tools there are uses for it that are illegal,” said Linn, a security consultant at Trustwave’s SpiderLabs. “We don’t outlaw screwdrivers and hammers because someone might use them for murder, though. We prosecute those people who use them illegally.”

A researcher named H.D. Moore began working on Metasploit in 2002. Moore, now 31, is the chief security officer with Rapid7, a security firm that sells a commercial version of Metasploit and helps offset the cost of maintaining the free system. A computer researcher and hacker based in Austin, Moore wanted to simplify the development of computer hacks known as exploits. To keep pace with growing numbers of criminal cyberattacks, he wanted to make security hacking, or “penetration testing,” more systematic.

Metasploit works by creating ready-made packages of computer code, known as “modules,” that can be downloaded from metasploit.com. Once they are launched, the tools can find network vulnerabilities and take control of the systems.

Metasploit also serves as something of a global clearinghouse of hacker knowledge, tools and practices. Because it is an “open source” system, it relies on contributions from experienced hackers. Its popularity has soared during the past several years. Starting with 11 exploits in 2003, Metasploit now has close to 1,000.

About 300 people in at least 20 countries have donated exploits so far. The contributors also collaboratively review the offerings to be sure they work effectively. Moore estimated that about 1 million people downloaded the free version during the past year, with about 5 million since its inception. It appears that about 200,000 penetration testers, including the U.S. military’s cyberwarriors, use it regularly, he said.

No one knows how many bad guys employ Metasploit and similar tools. Fears about that potential have been raised in Germany and elsewhere. But Moore said black-hat hackers typically rely on other tool kits that are less focused on research and more focused on swift, illegal break-ins.

Moore said the fact that criminals, spies and others with ill intent can access Metasploit is a necessary trade-off. To keep Metasploit up to date, hackers have to be able to contribute details about the newest vulnerabilities and attack methods.

An organization that keeps track of known vulnerabilities said it has documented more than 53,000, a number that rises every day.

“All we’re trying to do is put everyone on a level playing field,” Moore said.

‘A taste of things to come’

When Metasploit emerged, even veteran hackers marveled at its design and simplicity. A 2004 presentation about it at Black Hat Las Vegas, the annual hacker conference, was titled “Hacking Like in the Movies,” according to a 290-page online book called “Metasploit Toolkit” by David Maynor and
several other security researchers.

“The hall was packed to the gills. People stood in the aisles, and the crowd was spilling over to the main corridor,” the authors wrote. “Applause flowed freely throughout the session, and the consensus was clear, ‘Metasploit had come of age.’ But we should have known better. That was only a taste of things to come.”

The extraordinary thing about Metasploit is the digital architecture that streamlined what had been a laborious process of exploit development. That process invariably involved several steps for anyone, good or bad: the discovery of a software vulnerability; the analysis of the code to see whether the vulnerability could be exploited; the writing of the exploit itself, including the commands that tell a target system to open up to an intruder; and testing to ensure the exploit worked.

With Metasploit, all those steps are already done and packaged together with still other features, including tailor-made “payloads” that take effect and hand over control of a system after a hacker gets in.

Other systems have been created to ride on top of Metasploit and make it even easier to use. One called Armitage was created by Raphael Mudge, who was recently hired under contract by the Defense Advanced Research Projects Agency to develop new cybertools.

“Armitage recommends exploits and will optionally run active checks to tell you which exploits will work,” Mudge said in an Armitage tutorial. “If these options fail, use the Hail Mary attack to unleash Armitage’s smart automatic exploitation against your targets.”

In some cases, Moore said, researchers use the Metasploit framework to apply pressure on software vendors to improve the security of their products. If the vendors neglect to fix a known bug, the researchers write an attack module to spur them to act.

That happened this year when a group of researchers created attack modules for six industrial control systems, the computers that operate the power grid, water plants and other critical infrastructure.

“It forces the security vendors to take that vulnerability seriously,” Moore said. “And it forces the vendors responsible for that software to provide a patch or a work-around.”

Alan Paller, director of research at the Sans Institute, one of the world’s leading cybersecurity training organizations, said Metasploit contributors are playing a crucial role in highlighting the pervasive vulnerabilities in systems throughout cyberspace.

“They solve a critical problem for us,” Paller said. “They are necessary tools right now when much of the world is still in denial.”

No one knows how many illicit attack kits are sold to black-hat hackers. Offers appear every day across the Internet. Moore said exploit kits that employ “botnets” in criminal schemes often sell for up to $10,000.

A botnet is a network of computers that have been infected by malicious software and are controlled by bad guys. They often send spam, but they are also used to send malicious code, or malware, in coordinated attacks on networks.
Moore said that in several cases, the bad guys have used botnets to attack Metasploit as punishment for spurring fixes to widely attacked vulnerabilities.

“We do a good job killing bugs,” Moore said. “When the Metasploit adds a new attack, it instantly raises the visibility of that vulnerability.”

Many options

Robin Jackson sat in his Helena, Mont., office and prepared to launch his next hack. The target: a Chinese company’s Web site.

Jackson is a security researcher for a firm called WT Forensics. He said he also participates in informal networks of hacker-intelligence specialists who try to keep watch on the black hats and cyberwarriors across the globe.

He described his China effort as an exploratory “gray hat” hack to see if the target company’s Web page was vulnerable. He decided he would use a set of commands to make his attack seem as though it were coming from a computer in London. To penetrate the Web server, he would turn to the collection of tool kits he keeps on his computer.

In addition to Metasploit, Jackson relies on a number of other automated attack kits almost every day to do his job. There are many of them: Nmap scans the configuration of networks. John the Ripper and Hashcat crack passwords. The Social Engineering Toolkit combines automation with manipulation techniques to help hackers trick people into giving them access to networks.

A host of commercial systems, including a premium version of Metasploit, make it possible to attack multiple client machines at a time. A firm called Immunity, maker of a security tool kit called Canvas, recently released a related commercial system called Swarm. It enables security researchers to scan and attack up to a million servers an hour.

For this exploratory mission, Jackson decided to use a more focused free tool called Havij. With a few clicks on his keyboard, he directed Havij at the targeted Internet address in China. He typed “%Inject Here%” to launch the program.

Havij has been built to send thousands of permutations of commands to implement something known as an SQL Injection attack. Havij would keep hammering the targeted Web server until it sent a command that slipped by the server’s security.

A few years ago, Jackson would have had to type each attack command by hand. With Havij, he can launch the attack, sip his coffee and wait. “Unlike the manual process, Havij automatically does everything seamlessly and much more quickly,” he said.

For all their benefits, Jackson said, the kits are lowering the barriers to entry for inexperienced hackers. Criminal hackers and “hacktivists” can simply download the tool kit and then watch an instructional video on YouTube to get started.

Members of the hacktivists group Anonymous have used the system to target police and military networks. A group called Team GhostShell relied on it to compromise hundreds of Chinese Web sites.

“The Internet not only enables the distribution of hacking tools, but it also offers the hands-on
Hacking tool kits, available free online, fuel growing cyberspace arms race - The Washin...

instruction and training on how to use these,” Jackson said. “There are literally thousands upon
thousands of videos … which show the neophyte how to install and use these tools.”

Sponsored Links

LifeLock® Fraud Services
LifeLock® Credit Alerts For Fraud Protect Against Identity Fraud.
LifeLock.com

NFL Extra Points Card
Get Unbeatable Rewards & No Annual Fee w/ Your Official NFL Team Credit Card. Apply Today.
http://www.nflextrapoints.com

Trident University Online
Use Your Veteran Benefits To Get a College Degree Online at TUI!
www.Trident.edu

© The Washington Post Company
In cyberattacks, hacking humans is highly effective way to access systems

By Robert O'Harrow Jr., Published: September 26

The e-mails arrived like poison darts from cyberspace.

Some went to the Chertoff Group, a national security consulting firm in Washington. Others targeted intelligence contractors, gas pipeline executives and industrial-control security specialists. Each note came with the personal touches of a friend or colleague.

"Attach[ed] is a quote for the Social Media training we discussed," said one message sent on July 3 to the vice president of EnergySec, a federally funded group in Oregon that focuses on the cybersecurity of the nation’s power grid.

But like much of the digital universe, the e-mails were not what they seemed. They were cyberweapons, part of a devastating kind of attack known as "social engineering."

Emerging details about the e-mails show how social engineering — long favored by con artists, identity thieves and spammers — has become one of the leading threats to government and corporate networks in cyberspace.

The technique involves tricking people to subvert a network’s security. It often relies on well-known scams involving e-mail, known as "spear phishing," or phony Web pages. But such ploys now serve as
the pointed tips of far more sophisticated efforts by cyberwarriors to penetrate networks and steal military and trade secrets.

The e-mails this spring and summer appear to be part of a long-running espionage campaign by a hacker group in China, according to interviews with security researchers and documents obtained by The Washington Post. Some of the e-mails, including those sent to the Chertoff Group and EnergySec, were caught by suspicious employees. Others hit home.

"Multiple natural gas pipeline sector organizations have reported either attempted or successful network intrusions related to this campaign," officials at the Department of Homeland Security said in a confidential alert obtained by The Post.

The May 15 alert, by the department’s specialists in industrial control systems, said "the number of persons targeted appears to be tightly focused. In addition, the email messages have been convincingly crafted to appear as though they were sent from a trusted member internal to the organization."

Social-engineering attacks revolve around an instant when a computer user decides whether to click on a link, open a document or visit a Web page. But the preparation can take weeks or longer.

Serious hackers investigate their targets online and draw on troves of personal information people share about themselves, their friends and their social networks. Facebook, Twitter and other social media have become prime sources for the hackers, specialists said.

"Everybody has their trigger," said Bruce M. Snell, director of technical marketing at McAfee Security Systems. "A good social engineer will find that trigger."

Once malicious software code is delivered, it burrows in and hides in a targeted network. That code, known as malware, can lurk for years in intelligence or attack schemes that are sometimes known as "advanced persistent threats." Eventually, the code reaches back out to the hackers for instructions, often cloaking the communication through encryption or masking it to seem like innocuous Web browsing by an employee.

Over the past three years, most major cyberattacks on U.S. corporations have included social engineering, specialists said. That includes hacks of Google and security giant RSA. Researchers think that scores of attacks were designed by the same Chinese hackers who appear to be involved in the current e-mail campaign. Some U.S. officials think the hackers may have links to the Chinese military.

The Chinese are not the only ones using the technique. Cyberwarriors at the Pentagon receive social-engineering training for offensive and defensive missions, knowledgeable specialists said.

David Kennedy, a security consultant and former National Security Agency analyst, said he is amazed at the effectiveness of the techniques.

"I have done hundreds of these, and I have never been stopped," said Kennedy, who teaches social engineering to other security specialists. "It sounds horrible, but it works every single time."

**The human factor**

Social engineering works because it targets a vulnerable part of cyberspace that cannot be patched with technical fixes: human beings. People want to believe that their communication is safe.
In cyberattacks, hacking humans is highly effective way to access systems - The Washington...

"Because it goes at the human level, not at the technological level, we’re all vulnerable," said Joseph Nye Jr., a distinguished service professor at Harvard University who is on the board of advisers to the Chertoff Group. Nye said he has received at least six spear-phishing e-mails purporting to be from the Chertoff Group. He said he deleted them all, but he added, "Every once in awhile, one of these will get by you."

The explosive growth of cyberspace has created a fertile environment for hackers. Facing the flood of e-mail, instant messages and other digital communication, many people have a hard time judging whether notes or messages from friends, family or colleagues are real. Many don’t even try. Hackers are so confident about such permissiveness that they sometimes begin their attacks in social media three or four steps removed from their actual targets. The hackers count on the malicious code spreading to the proper company or government agency — passed along in photos, documents or Web pages.

"This is the next evolution of social engineering, where victims are researched in advance and specifically targeted," said a recent Internet threat report by Symantec, a computer security firm. "The very nature of social networks makes users feel that they are amongst friends and perhaps not at risk. Unfortunately, it’s exactly the opposite and attackers are turning to these sites to target new victims."

At the same time, technology is transforming social engineering. One online data-mining service favored by hackers — as well as by security researchers and law enforcement — works much like a laser-focused Google. The automated system, called Maltego, enables users to quickly bring together and analyze disparate details about people from all corners of cyberspace, showing an individual’s links to friends, family, work associates and personal interests.

"None of these steps are particularly difficult to code or do by hand. But doing it by hand is painful," said Roelof Temmingh, founder and managing director of Paterva, the small South African company that sells the service. "Maltego can do all of this in a flash."

Temmingh demonstrated Maltego’s utility not long ago by looking for a person to target at Fort Meade, home to the super-secret NSA. He typed in Fort Meade’s latitude and longitude and searched for Twitter users. In a couple of steps, Maltego quickly delivered the name of a person who tweeted at the Fort Meade location.

With that, Maltego searched MySpace, a dating Web site and other resources to build a rich profile: a young Army private who served in South Korea, likes to smoke and drink, divorced and looking for a "serious relationship." She likes Harry Potter movies and "The Cosby Show." Maltego also turned up her name, address and birthdate.

**Building a tool kit**

In 2009, David Kennedy began digging deep into corporate security for a Fortune 1000 company as a penetration tester, identifying flaws that hackers could exploit. He wanted to know whether employees could be duped into clicking on unknown documents or handing over confidential information over the phone. Most of them could.

Kennedy concluded that social engineering was "the next biggest attack vector." He teamed up with a nonprofit organization called Social-Engineer.org to develop products that would make security testing more effective.

The result is known as the Social Engineering Toolkit. Its many applications can identify targets and
deliver attack payloads, secretly, like digital stealth missiles. The tool kit also provides ready-made code for attacks.

In an irony of the digital age, the same tools are available for free to attackers.

“Can a bad guy take all this and get better? Sure. . . . But that is not the intended goal,” said Chris Hadnagy a founder of Social-Engineer.org and author of the book “Social Engineering: The Art of Human Hacking.” “What we are doing is trying to weaponize people to be protected against this threat.”

Kennedy described one effective approach involving a tool that creates instant copies of real Web pages and embeds them with malicious code. In an e-mail, the attacker could pose as an executive of a company, seeking help from an IT department employee. The attacker has studied the employee and knows he is new to the company and probably eager to please his superiors.

In a phone call that appears to be coming from within the company, the attacker asks the IT staffer why a certain Web page won’t open. The attacker directs the staffer to the bogus Web page. The intrusion occurs the moment the IT staffer visits the page.

“I find that leveraging human compassion is generally the best way to gain what I want,” Kennedy, now president of TrustedSec, said in a recent seminar.

**A tailor-made attack**

The current intrusion campaign began in December, possibly earlier. That’s when analysts think the attacks first started against gas pipeline company executives. With some study, it became clear that the e-mails were part of a sophisticated campaign. Only certain executives were singled out for attention. The e-mails were tailored to them.

The attackers were relentless, launching e-mails on at least 13 days. They also were creative. Attached to the e-mails were documents covering a variety of subjects that might be of interest to the executives: the U.S. debt crisis, Adobe updates, iTunes help and an analysis of the presidential election.

The true scope of the campaign started to become apparent in June, after cybersecurity researchers at a security firm called Digital Bond received one of the phony e-mails. The Digital Bond researchers specialize in industrial-control computers that operate power plants and other critical infrastructure.

The note, which appeared to be coming from their boss, Dale Peterson, was filled with technical jargon. “Details are available at: Leveraging_Ethernet_Card_Vulnerabilities_in_Field_Devices.pdf Download it and have a look,” the e-mail said.

The intrusion failed in part because the attackers slipped up and because a Digital Bond researcher was alert. The e-mail was signed “Peterson.” But the security researchers knew that their boss uses his first name on e-mail, not his last.

Other security researchers asked to review the situation found the attachments were not actually .pdf documents but “executable files” that deposited “Trojan horse” code when a computer user clicked on them, said Jaime Blasco, security lab manager at AlienVault, who reviewed the attack.

Blasco and his partner, Ruben Santamarta of the security firm IOActive, found the hackers had used multiple Web server computers to give instructions to the malicious code. The electronic trail on those
servers led to other victims, including the Chertoff Group; NJVC of Vienna, Va., a contractor for the National Geospatial-Intelligence Agency; and the National Electrical Manufacturers Association (NEMA) in Arlington County, which represents companies that make components for power grids.

Officials at NJVC and NEMA acknowledged the attacks but said employees prevented network intrusions. Department of Homeland Security officials declined to discuss the episodes.

The scope of the attacks expanded in July, when the cybersecurity group EnergySec was hit. EnergySec President Patrick Miller also reached out to Blasco for help. Based on evidence, it appeared to be the same attackers: a group of Chinese hackers that had been using social engineering for nearly a decade to break into systems across the globe with impunity.

Cyber-researchers have dubbed them the Comment Crew or Comment Group. The name stems from the fact that hackers include attack commands in the comments that programmers typically include in HTML code to document their goals or make notes of changes.

The Comment Crew has become notorious for using simple social-engineering techniques, including well-crafted e-mails, in elaborate hacks that breach security, load “remote access tools,” or RATs, and siphon off oceans of data from victims.

Though it is sometimes impossible to definitively identify hackers, because of the hall-of-mirrors nature of cyberspace, they often leave behind compelling digital evidence. Researchers said the IP address of a Web server and a particular method of writing HTML comments links the attacks on the gas pipeline executives to those against the Chertoff Group and others. It also links the current campaign to a series of earlier devastating attacks by the Comment Crew, dubbed Operation Shady RAT.

Those intrusions compromised hundreds of systems over at least five years, including federal agencies, defense contractors and the United Nations, according to studies by McAfee and the Dell SecureWorks Counter Threat Unit.

“The above patterns of attack are very similar to attacks carried out by the actors responsible for the Shady RAT campaign,” said Ned Moran, a researcher at the nonprofit Shadowserver Foundation who also analyzed the attack on Digital Bond.

Joe Stewart, director of malware research at the Dell SecureWorks Counter Threat Unit, estimates the group has at least 100 members who work at specific tasks such as social-engineering research, malware development and the processing of stolen information. In essence, the Comment Crew has made a business of cyber-espionage. Their activity online shows they typically work 9 to 5 — Shanghai time — and take off Chinese holidays.

Stewart and others say Chinese hackers have been using a troubling variation of social engineering called a “watering hole” attack. Instead of sending e-mails with links — something that some security-conscious computer users now avoid — they try to entice wary victims to visit familiar, authentic Web sites that have been secretly loaded with attack code. Think of a lion near a watering hole.

One ploy involves an e-mail announcement of online coupons for half-price drinks or food at a favorite bar. The attack comes when the victims visit the Web site seeking the coupons and unwittingly download the malware.

In a new report, Symantec researchers said some hackers are simply co-opting Web pages popular in

http://www.washingtonpost.com/investigations/in-cyberattacks-hacking-humans-is-highl... 11/19/2012
In cyberattacks, hacking humans is highly effective way to access systems - The Washing...

...one certain industries, such as the energy sector, and waiting for victims to arrive.

With enough money, focus, malware and social-engineering skills, “anybody can get into anyplace,” Stewart said. “The most careful person is not going to have a defense against it.”

**Sponsored Links**

**LifeLock® Fraud Services**  
LifeLock® Credit Alerts For Fraud Protect Against Identity Fraud.  
LifeLock.com

**NFL Extra Points Card**  
Get Unbeatable Rewards & No Annual Fee w/ Your Official NFL Team Credit Card. Apply Today.  
http://www.nflextrapoints.com

**Looking for a new Home?**  
Use CNNMoney's free Home Search tool to find thousands of listings  
http://realestate.money.cnn.com

© The Washington Post Company
Tridium’s Niagara Framework: Marvel of connectivity illustrates new cyber risks

By Robert O’Harrow Jr., Published: July 11

John Sublett and his colleagues had an audacious, digital-age plan. They wanted to use the Internet to enable businesses to manage any kind of electronic device, anywhere on the planet, through the computer equivalent of a universal remote control. In 1996, nothing like it had been seen before.

“We said, ‘Hey, there’s this cheap network, ready to use,’” Sublett recalled.

Their company, Richmond-based Tridium, would succeed — but with far-reaching implications for the security of the online universe known as cyberspace.

Tridium’s driving technology, 4 million lines of software code called the Niagara Framework, is a marvel of innovation. With the click of a mouse, Niagara enables plant managers to view video streams, high-rise superintendents to operate air conditioners and elevators, security officials to track personnel inside U.S. military facilities, and nurses to monitor medical devices in hospitals.

At least 11 million devices and machines in 52 countries, including security and surveillance systems in homes, have been linked to the Internet through Niagara, most of them in the past two years. But behind that success is a looming threat: an unknown number of Niagara-run networks are vulnerable to attacks from hackers, an examination by The Washington Post has found.
Last week, after more than a month of conversations with The Post, the company in a confidential security bulletin warned customers about the vulnerabilities and described ways to mitigate them.

“We’re not going to say Niagara is secure,” Sublett said in an interview. “We try to soften it and say we’re trying to make it as secure as possible.”

Tridium’s story illustrates the unintended consequences of the world’s rush to connect machines and devices in cyberspace. It also demonstrates how even small missteps in writing software or configuring systems can have huge implications. In cyberspace, determined hackers routinely transform obscure gaps into major security holes.

Over the past two years, hackers and cyberwarriors who once focused primarily on traditional computers and networks have put control systems in their crosshairs, damaging machinery, stealing information from networks and spying on facilities. Warnings from the Department of Homeland Security about the threats have become a drumbeat, while officials at the Pentagon and the White House consider them a national security priority.

After discussing Tridium with a Post reporter, a pair of security researchers decided on their own to zero in on Niagara and discovered gaps that would enable hackers to download and decrypt user names and passwords. The researchers, Billy Rios and Terry McCorkle, shared their findings with The Post and reported them to cybersecurity officials at the Department of Homeland Security, who recommended several measures to Tridium, including better security training for customers.

“There are hundreds of thousands of installations on networks, including [Defense Department] installations and Fortune 500 firms,” said Rios, a 34-year-old security researcher and a co-author of “Hacking: The Next Generation,” a handbook for security experts. “These customers have no idea they are exposed.”

In interviews, Sublett defended Niagara’s security, saying it follows industry “best practices” and “is basically secure.” He said Tridium has long recommended, to customers who asked, that users protect against intrusions by placing Niagara behind more-secure “virtual private networks.”

Sublett said executives learned about the vulnerabilities almost a year ago, when a Niagara customer that uses the software to manage Pentagon facilities turned up issues in an audit. He said Tridium is working on fixes. The firm also is doing more to train customers about security than it has in the past, he said.

“We’re committed to making our framework more secure,” Sublett said. “And we know it’s our responsibility to educate our community.”

No longer off the radar

For more than a decade, few people gave much thought to the security of commercial control systems on the Internet.

Tridium executives said attacks seemed unlikely, because hackers had not traditionally targeted such systems. In interviews, the executives said they and their customers generally assumed that control systems were buffered somewhat by their obscurity.

Rios and other “white hat” hackers — those who seek to improve security by exposing flaws — noticed Niagara systems popping up online in recent years, as office buildings, apartment complexes and other
facilities automated heating systems, security and other operations. One researcher documented thousands of “portals” online. Others shared details about Niagara locations and speculated about their security.

But the interest did not take hold beyond a small cadre of security specialists, because few people grasped the implications of Tridium’s business and its expanding reach.

Commercial control systems rely on computer software, microprocessors and networks. They do not have to be as quick or as finely calibrated as the industrial control systems that run power generators, manufacturing equipment and other heavy machinery. But they are far more numerous.

In 1996, Sublett and five colleagues wanted to give customers options to connect a wide variety of devices into a single network. At the time, devices had to be controlled separately by each manufacturer's software.

The team formed Tridium and designed Niagara to leverage the technology that is at the core of the Web. The Web uses the universal Hypertext Transfer Protocol, or HTTP, to facilitate computer-to-computer communication over the Internet.

In 1999, Tridium introduced the software framework to the market. Niagara permitted other companies to tailor the software to incorporate any device. At its core, Niagara serves as a kind of middleman that transforms the electronic babble of every network-connected device into a single manageable language.

Like the Web, Niagara was easy to use, and word spread in the world of control systems. Over the next few years, so many smaller companies began licensing Niagara to use in building automation projects that the big makers of commercial control systems began to follow suit.

In 2005, as the notion of connecting machines to cyberspace was gaining momentum, Honeywell International bought the company for an undisclosed amount and allowed Tridium to operate independently. Sales of the system soared, and Tridium’s promotional materials include examples of Niagara’s growing presence around the world.

In Chicago, the Niagara software manages heating, lighting, security and more for two federal government buildings that house the FBI, the Drug Enforcement Administration, the U.S. Attorney’s Office, the Internal Revenue Service and other agencies.

In Dubai, in the United Arab Emirates, managers of the 53-story 21st Century Tower apartment complex use the software to control fire detection, security sensors, air conditioning and myriad other operations.

At Singapore’s Changi Airport, Niagara helps manage more than 110,000 devices and sensors. The James Cook University Hospital in Middlesbrough, England, relies on Niagara to manage everything from “critical medical systems” to elevators, security, lighting and kitchen refrigeration.

Some Defense Department facilities in the United States also depend on Niagara. That includes the giant Tobyhanna Army Depot in Pennsylvania, which uses Niagara to control boilers. Some military installations use Niagara to provide surveillance and access control at “high security” facilities, said Marc Petock, Tridium’s vice president for global marketing and communications.

Growing numbers of home-automation companies are using Niagara to enable homeowners to control lighting and security systems.
One of the most widespread uses of Niagara involves about 575 Wawa convenience stores nationwide, where the software connects oven doors, gasoline pumps, exterior lights, freezers and security cameras, all controlled or monitored from a Wawa command center.

Wawa embodies Tridium’s lofty ambitions, as Petock describes them: “Any device, any system, any network, any protocol from anywhere at any time.”

**Inside Niagara**

Rios first noticed Niagara more than a year ago, while working on a security project. He became intrigued about the framework while attending a security conference in January, as he drank beers and smoked a cigar on a veranda at a conference center in Miami.

Rios is a former Marine captain who served in Iraq with a signals intelligence unit and later as an information assurance analyst at the Defense Department, helping to protect networks. Since then, he has held senior security positions at Microsoft and Google.

On their own time, Rios and his research partner, McCorkle, also a corporate security specialist, have made a specialty of finding vulnerabilities in industrial and commercial control systems. The two have been credited with reporting at least 25 serious vulnerabilities to cybersecurity officials at the Department of Homeland Security and vendors.

Rios was troubled by what he was hearing about Niagara in Miami. Another researcher described how he had mapped thousands of Niagara-driven networks. He said they were linked directly to the Internet even though many apparently required only user names and passwords for access. To a hacker such as Rios, that was virtually no security at all.

Following the conference, after a Post reporter called and shared new details about Tridium — including the use of Niagara by the Pentagon and other federal agencies — Rios decided to take a closer look.

On Jan. 26, sitting in his family’s San Jose living room and working on a laptop, Rios began to work. He created an account on a Tridium Web site devoted to helping users, lurking quietly as he read complaints and recommendations. The comments from users helped him to construct a “mental map” of how the software worked.

“I’m learning about its weaknesses, and I’m learning about the common configurations that I’ll likely see in the wild,” he said later.

A key moment came when someone in the online forum referred to technical manuals and a Web address where they were located. Rios and McCorkle downloaded the manuals and pored over them for clues. Rios saw a reference to a Niagara demonstration site online and turned his attention there.

As he toyed with the demo and hunted for an exploit, his insights gleaned from the manuals crystallized. “Within five minutes, I’ve found what I’m looking for,” Rios later wrote in an e-mail to The Post. “I find a flaw that gives remote attackers the ability to download all the user names and passwords for all the users on the Niagara server. I test it against the demo server ... it works. I test it against a couple of other places ... it works. The attack is trivial and very reliable.”

The exploit, well known in the hacker world, is called a directory traversal attack. It enabled Rios to turn the Web’s core function — the communication protocol that is intended to make everything easier — to
his advantage. With some deft alterations to the Niagara Framework’s Web address, he was able to order
the framework to perform certain tasks. One of them was to electronically hand over a “configuration
file,” which happens to contain user names, passwords and other sensitive material.

By the time he was finished, it was 3 a.m. on Saturday, Jan. 28. Rios crafted a technical note about his
exploit to cybersecurity officials at DHS and, after encrypting the message for security, sent it off. “All
total, it took me 2 days to go from zero knowledge to remote password theft,” Rios wrote.

The passwords Rios had grabbed were scrambled for security by a mathematical formula called a
“hash.” But that offered limited protection. Automated computer tools can crack the hashed passwords
with relative ease. (In a recent attack on LinkedIn, a social-networking site, hackers made off with
6.5 million hashed passwords and immediately began cracking them.) “Once the passwords are
decrypted, you can simply log in to the Niagara Framework as any user you desire,” Rios said.

A senior cybersecurity official at DHS acknowledged that the department had received Rios’s
information and had talked to Tridium.

Tridium officials attributed the demo vulnerability to an employee who they said set it up incorrectly.
They said some Niagara Framework users have also misconfigured their systems. Other users have
never bothered to take secure measures, such as using a hard-to-hack virtual private network.

Sublett said the company intends to change the location of the configuration file to make it harder for
hackers to find. Tridium also is trying to figure out the best way to change the framework’s default
security settings “so it’s not as easy to make a mistake.” And it is going to improve the hash that
scrambles passwords because “it’s not as strong as it should be,” Sublett said.

The company, still in talks with DHS officials, has begun a push to better communicate to Niagara users
about the security risks in cyberspace. The security bulletin last week was part of that process.

“We’re not out there claiming we are bulletproof secure,” Sublett said. “Nobody is 100 percent secure.”

Sponsored Links

LifeLock® Fraud Services
LifeLock® Credit Alerts For Fraud Protect Against Identity Fraud.
LifeLook.com

NFL Extra Points Card
Get Unbeatable Rewards & No Annual Fee w/ Your Official NFL Team Credit Card. Apply Today.
http://www.nflextrapoints.com

Looking for a new Home?
Use CNNMoney’s free Home Search tool to find thousands of listings
http://realestate.money.cnn.com

© The Washington Post Company

http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-co... 11/19/2012
Cyber search engine Shodan exposes industrial control systems to new risks

By Robert O'Harrow Jr., Published: June 3

It began as a hobby for a teenage computer programmer named John Matherly, who wondered how much he could learn about devices linked to the Internet.

After tinkering with code for nearly a decade, Matherly eventually developed a way to map and capture the specifications of everything from desktop computers to network printers to Web servers.

He called his fledgling search engine Shodan, and in late 2009 he began asking friends to try it out. He had no inkling it was about to alter the balance of security in cyberspace.

"I just thought it was cool," said Matherly, now 28.

Matherly and other Shodan users quickly realized they were revealing an astonishing fact: Uncounted numbers of industrial control computers, the systems that automate such things as water plants and power grids, were linked in, and in some cases they were wide open to exploitation by even moderately talented hackers.

Control computers were built to run behind the safety of brick walls. But such security is rapidly eroded by links to the Internet. Recently, an unknown hacker broke into a water plant south of Houston using a default password he found in a user manual. A Shodan user found and accessed the cyclotron at the
Lawrence Berkeley National Laboratory. Yet another user found thousands of unsecured Cisco routers, the computer systems that direct data on the networks.

“There’s no reason these systems should be exposed that way,” Matherly said. “It just seems ludicrous.”

The rise of Shodan illuminates the rapid convergence of the real world and cyberspace, and the degree to which machines that millions of people depend on every day are becoming vulnerable to intrusion and digital sabotage. It also shows that the online world is more interconnected and complex than anyone fully understands, leaving us more exposed than we previously imagined.

Over the past two years, Shodan has gathered data on nearly 100 million devices, recording their exact locations and the software systems that run them.


Homeland security officials have warned that the obscurity that had protected many industrial control systems was fast disappearing in a flood of digital light.

“This means that these delicate [control computers] are potentially reachable from the Internet by malicious and skilled adversaries,” a Department of Homeland Security paper concluded in 2010.

The number of intrusions and attacks in the United States is rising fast. From October to April, the DHS received 120 incident reports, about the same as for all of 2011. But no one knows how often breaches have occurred or how serious they have been. Companies are under no obligation to report such intrusions to authorities.

A weak link in the system

Industrial control systems are the workhorses of the information age. Like other computers, they run on code and are programmable. Unlike laptops, smartphones and other consumer technology, they’re stripped down and have little style or glitz.

Costing as little as a few thousand dollars and up to $50,000, they’re often housed in plain metal boxes with few lights or switches. Control systems now open and shut water pipes, regulate the flow of natural gas, manage the production of chemicals, and run data centers, power-plant turbines and commuter trains.

The control computers collect data from electronic sensors, analyze it and send it on to desktop computers that serve as the “human-machine interface.” They afford managers precise and remote control of the machinery.

The most far-flung and powerful of these networked systems are called supervisory control and data acquisition, or SCADA. They give companies central control of large numbers of pumps, generators, oil rigs and other operations.

The allure of long-distance network control is hard to resist. Manufacturers of control computers have promised that such networks can cut costs by reducing the number of workers in the field. Siemens Industry Inc., a leader in the field, said in a recent marketing brochure that it is “more important than ever” to adopt control devices “to respond to the increasing international competitive pressure.”
The systems are often hardened against weather or tough conditions and can run nonstop for months or years. But many were designed for another era, before the mesh of networks reached into every corner of the globe, and some of the systems rely on outdated hardware and software.

A recent examination of major control systems by six hacker-researchers working with the security firm Digital Bond found that six of seven devices in the study were riddled with hardware and software flaws. Some included back doors that enabled the hackers to download passwords or sidestep security completely.

Researchers found that one machine made by General Electric, the D-20, uses the same microprocessor installed in Apple computers two decades ago. The company that made its operating software stopped updating it in 1999. It is often shipped to customers with no meaningful security. “Security is disabled by default,” the manual says. “To log in, enter any name; you do not need a password.”

In a statement to The Washington Post, General Electric said: “The D-20 was designed for deployment in a layered security environment, in which asset owners and operators employ a range of measures to prevent, detect and respond to intrusions. GE actively works with our customers to design and support those security measures.”

The company added that the software for the machine “is designed to be secure and includes a layer of password-protection, which can be activated if the customer chooses to do so.”

Other machines had flaws that enabled the researchers to take control through electronic back doors.

In January, Digital Bond said the results were “a bloodbath, mostly.”

“Most of the guys were able to hack their controllers in a single day,” said K. Reid Wightman, a Digital Bond security researcher and former Pentagon cyberwarrior. “It’s just too easy. If we can do it, imagine what a well-funded foreign power could do.”

The owners of control computers long assumed that few outsiders understood or cared how power plants and other facilities worked. They also figured the systems were safe within their facilities, disconnected from outside networks.

But like much of the rest of the world, the systems were rapidly being linked to global networks, often through indirect connections. Many of those connections came as executives sought more refined detail about their operations. With few exceptions, corporate networks used by executives are linked in some way to the Internet.

Because of the strange nature of cyberspace, even an employee passing through a plant with a wireless connection on a laptop can create a temporary data link that exposes control systems to intruders.

“They have sort of connected through osmosis,” said Marty Edwards, a senior cybersecurity official at the Department of Homeland Security. “What we have done is connect to everything.”

An accidental discovery

The idea for Shodan came to John Matherly in 2003, when he was a teenager attending community college in California. Obsessed with the digital world, he named his project after a malevolent character in a video game called System Shock II. The character, Sentient Hyper-Optimized Data Access

http://www.washingtonpost.com/investigations/cybersearch-engine-exposes-vulnerabilities... 11/19/2012
Network, or Shodan, is an artificial intelligence entity that thinks it is a goddess and sets out to eradicate humans.

Matherly, who grew up in Switzerland, toyed with his system for years as he earned a degree in bioinformatics from the University of California at San Diego and built his career as a programmer, data miner and Web developer. His early Shodan versions found only hundreds of devices a day on the Web, and the information was not searchable. After devoting months to the project in 2009, he made a breakthrough, solving the search problem and locating many more devices.

When he launched his first live version of the program, in November of that year, he thought it might catch on with software makers who wanted to know about the systems being used by potential customers. On his Web site, Matherly described his program as “the world’s first computer search engine that lets you search the Internet for computers. . . . Find devices based on city, country, latitude/longitude, hostname, operating system and IP.”

The Shodan software runs 24 hours a day. It automatically reaches out to the World Wide Web and identifies digital locators, known as Internet protocol (IP) addresses, for computers and other devices. The program then attempts to connect to the machines. If a connection is made, Shodan “fingerprinted” the machine, recording its software, geographic location and other data contained in the identification “banner” displayed by devices on the Internet.

Such identifying information is called “metadata” — and it’s far more common, useful and problematic than anyone had realized. Shodan compiles the information in Matherly’s servers — about 10 million devices every month now — and makes it almost as easy to query online as a Google search.

At first, the Shodan discoveries seemed trivial: devices commonly linked to networks such as printers and Web servers. But as queries became more sophisticated, troubling findings started emerging. One researcher using the system found that a nuclear particle accelerator at the University of California at Berkeley was linked to the Internet with virtually no security. Another identified thousands of data routers — the devices that make networks possible — open to anyone. Because they required no passwords, they could be taken over with ease.

"It was only after nearly a year that individual researchers began digging deeper through the Shodan data to locate devices that weren’t part of the known, discovered Internet,” Matherly said. “Water-treatment facilities, power plants, particle accelerators and other industrial control systems had been hidden from traditional search engines.”

As the dimensions of the challenge posed by Shodan became clear, the DHS Industrial Control Systems Cyber Emergency Response Team issued a stark warning in October 2010, noting “the increased risk” of brute-force attacks on “systems available on the Internet.”

The alert recommended placing all control system assets behind firewalls, using secure remote-access methods and disabling default passwords.

A researcher at Cambridge University, Eircann Leverett, used Shodan to identify more than 10,000 control computers linked to the Internet, many of them with known vulnerabilities. Leverett concluded that many operators had no idea how exposed they were — or even realized that their machines were online.

"This could be used to carry out remote attacks on selected devices or identify networks for further

In the United States, security experts Billy Rios and Terry McCorkle said this spring that their research suggests the situation is worse than even Leverett demonstrated. Rios, who works for Google, and McCorkle, who works for Boeing, are both Shodan users who study control systems on their own time.

“The number of control systems on the Internet is far greater than anybody realizes,” said McCorkle, who along with Rios recently discussed control computer vulnerabilities at the National Defense University at Fort McNair. “These systems are insecure by their nature.”

Matherly said he wants his search engine used to improve security. But he said it can be used to shred it as well.

“Shodan has lifted the barrier. There’s no going back,” Matherly said. “Once you shed light on it, you can’t go back into hiding.”

A history of digital attacks

One story from the Cold War shows that cyberattacks on control systems have been in the imagination for a long time. Though some details are hard to confirm, it describes an attack that experts believe could happen today.

In 1981, a Soviet KGB colonel who became a spy for France, code name Farewell, shared Soviet plans to use a Canadian front company to secretly acquire technology to automate the Trans-Siberian gas pipeline, according to “At the Abyss: An Insider’s History of the Cold War,” by Thomas Reed, a former Pentagon official. Tipped off by the French, U.S. officials set up a front company to sell the technology, but only after they made some undetectable alterations to the computer code.

The alterations eventually “reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds,” Reed wrote two decades later. “The result was the most monumental non-nuclear explosion and fire ever seen from space.”

A KGB veteran later disputed the account. A document on the CIA’s Web site confirmed only that “contrived computer chips” were provided to the Soviets and “flawed turbines were installed on a gas pipeline.”

Evidence of the threat to control computers mounted.

In 1997, a teenage hacker using a personal computer and a dial-up connection shut down part of a telephone network in Worcester, Mass., cutting off the local airport’s air-traffic-control communications.

In 2000, Vitek Boden, a supervisor at a technology firm in Australia, was bitter that he did not get a job with the Maroochy Shire Council, according to Joseph Weiss, author of “Protecting Industrial Control Systems From Electronic Threats.” Using a radio transmitter, Boden launched an attack against a wastewater-treatment system in Queensland, remotely accessing the control systems and releasing hundreds of thousands of gallons of raw sewage into local streams and parks. He was sentenced to two years in jail.
“Marine life died, the creek water turned black and the stench was unbearable for residents,” an Australian Environmental Protection Agency official said later.

In 2007, skeptics still claimed that the threat of cyberattacks on real-world machinery was theoretical. In a demonstration called Project Aurora, the Department of Homeland Security along with power industry officials decided to test the theory themselves.

In the end, many doubters were silenced.

The target was a 5,000-horsepower diesel engine, the kind of machine that often serves as a backup generator for manufacturers and large organizations. Engineers at the Idaho National Laboratory hacked into the generator’s embedded control computer through a network. By repeatedly triggering circuit breakers, they created massive torque on the machinery, which eventually started to shake, smoke and tear itself to pieces.

Mark Zeller, who specializes in industrial power systems at Schweitzer Engineering Laboratories Inc., said the Aurora Project set off a scramble in the power industry to identify links to cyberspace and improve “electronic” perimeter security.

Those efforts include assessing the links between control systems and networks and creating layers of defenses against intruders. In some cases, that means creating “air gaps” — physical separations that cannot be breached by wireless connections — between networks and control systems along with stronger password protection.

“They have really taken this electronic security perimeter thing seriously,” Zeller said. “It’s a big issue now.”

At the same time, the DHS has stepped up its efforts, including providing advice and assistance to industries to reduce cyber-risks.

The government now routinely issues alerts about new threats to control systems. Alerts are also issued by a private industry group, the North American Electric Reliability Corp., or NERC, the organization of electrical grid operators in the United States.

Three weeks ago, NERC said that control computers on the Internet “face increased exposure” because of Shodan and hacking tools. The NERC alert said that “it is possible that hackers or hacktivist groups may cause sporadic component failures as they identify and interact with these devices.”

A sophisticated new virus called Flame, apparently aimed at intelligence collection against Iran, was revealed last week, underscoring anew the threats in cyberspace. But the most powerful and ingenious cyberattack ever publicly disclosed involved industrial control systems in Iran. Called Stuxnet when its code was discovered on the Internet in the summer of 2010, the attack alerted the world to the true potential for attacks on critical infrastructure.

Last week, the New York Times reported that Stuxnet was part of a U.S.-Israeli covert operation against Iran approved by President Obama. Stuxnet targeted a control computer called an S7 produced by Siemens and used by the Iranian government to operate centrifuges in the process of enriching uranium.

The malicious code designed to attack the machines was included as payload in a package of software called a computer “worm.”
The worm was launched into the Internet and spread rapidly around much of the world, like a virus during flu season. But most of the computers and systems infected were in Iran.

The worm code was designed to self-replicate. Investigators said it apparently infected flash drives in Iran, helping it jump from networks to unconnected computers at the Iranian nuclear processing facility in Natanz.

Stuxnet took advantage of four unknown software flaws, or zero days, to crack through security in a variety of computer systems. The attack code eventually directed the S7s to operate uranium-refining centrifuges at speeds beyond their tolerances while sending misleading data to monitors showing that all was well.

It was brilliant and devastating. Analysts believe that hundreds of centrifuges were damaged, though no one outside the operation knows for sure.

"The real-world implications of Stuxnet are beyond any threat we have seen in the past," said the authors of an analysis of the worm issued by Symantec, a computer security firm. "Stuxnet is the type of threat we hope to never see again."

Among those shaken to the core was Siemens.

"Stuxnet marked a turning point for the entire automation industry, turning theoretical problems into headlines," Raj Batra, president of the industry automation division at Siemens, told The Post.

**Exploiting flaws**

News of Stuxnet jolted hackers around the world like a double shot of espresso, waking them up to the once-obscure world of industrial control systems.

One of them was Dillon Beresford, an energetic hacker and security consultant in Texas. He read an article about the attack in Wired magazine.

"It inspired me," Beresford said. "I wanted to disprove that it would take a nation-state to pull this off."

"I’m like, no, I’m going to do this in my living room."

Beresford wasn’t just being brash. He had found zero-day vulnerabilities over the years. "At the end of the day, it’s all just code," he said.

Starting in January 2011, Beresford worked almost nonstop for two months. He focused on the Siemens S7 line of controllers.

Like any good hack, it started with research. Beresford found an online "coding library" run by a German researcher. It contained source code for a wide variety of computers, including the S7s. Night after night he studied, focusing in particular on what is known as the machine’s communications protocol.

He discovered the protocol was designed to make it easier for machines to communicate with the Internet. Security was an afterthought.
Beresford persuaded his boss at the time — a manager at NSS Labs, a security firm — to buy him four of the industrial control systems for thousands of dollars each. “If you do find something, let people know you’re from NSS,” his boss told him.

The devices came mounted on heavy boards, ready for testing. The S7 is a plain rectangular metal container with heat vents and ports for cables, about the size of a large shoe box.

Beresford set them up on his workbench in the bedroom of his apartment in suburban Austin. He connected them to his laptop and began to hunt.

“I was up every night until 5 a.m.,” he said. “I love to write code.”

Several weeks into his experiments, Beresford made the first of several discoveries of flaws in the S7s. One of them took advantage of the fact that the protocol did not encrypt its communication with other networks, allowing a hacker to easily read and steal the “plain text” passwords.

Beresford said the protocol was created by designers who assumed the machines would operate behind the safety of an “air gap” between them and open networks. At the time, no one anticipated the use of thumb drives to close such gaps, as in the Stuxnet attack.

He also found a digital back door that enabled him to read the device’s internal memory, including the password stored on the device.

In May 2011, Beresford sent his findings to the DHS. The feds studied his work and confirmed it. In an alert issued on July 5, the agency announced it was working with Siemens on the S7 vulnerabilities.

“I crushed it,” he said. “All average guys, your typical hacker, could very easily replicate this.”

Since then, using his Shodan account, Beresford has found more than 100 S7s online, all of them potential targets.

Batra of Siemens acknowledged the vulnerabilities and said the company is working hard to address them. The company last week announced it is offering new security enhancements for its industrial control systems.

“Siemens’s automation products are rigorously tested with regard to industrial security and yet must be designed to also balance the requirements of open industrial solutions, which drive productivity,” he said. “There will never be an endpoint when it comes to industrial security threats, but companies can better protect their systems by staying up to date with the research community, following the guidance of governmental agencies, and by working with responsible, technologically innovative vendors like Siemens.”

**Something to prove**

Other hackers also began turning their attention to industrial control computers after hearing about Stuxnet.

One of them, an anonymous hacker who calls himself pr0f, is a bright, unemployed 22-year-old who favors hoodie sweatshirts and lives in his parents’ home somewhere overseas. He is among the growing numbers of Shodan users.
After studying control systems in the wake of Stuxnet, he thought the insecurity of the devices seemed crazy and irresponsible.

“Eventually, somebody will get access to a major system and people will be hurt,” he later said. “It’s just a matter of time.”

He vowed to prove how easy it was to get in. On Nov. 17, he saw an article online about an apparent industrial control system attack in the United States. The article said a hacker in Russia had apparently destroyed a pump in a water utility in Springfield, Ill.

Pr0f had been expecting something like this, but he was incredulous when he read a statement in the story from a DHS official.

“At this time there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety,” the statement said.

The hacker fumed: How could Homeland Security play down something so important?

“It was the final straw,” pr0f said. “I was angry. I said, ‘Yep, let’s do something.’”

The Springfield episode turned out to be an accident not connected to Russia, but he did not learn that until later. Impulsively, he began programming his computer to search the Internet for a Siemens S7 controller. The first one he found just happened to be an S7 in South Houston, a small town thousands of miles and an ocean away from where he sat.

The hacker navigated to the machine’s Internet address. When prompted to identify himself as an approved operator, he knew just what to do, because he had read the manual. He typed in the default password: three simple digits. A moment later, he was at the controls of a water plant that serves 16,000 Texans.

“This required almost no skill,” the young man wrote online a short time later, using an e-mail address in Romania to cloak his identity.

The S7 was installed when the town upgraded its water plant more than a decade ago. That was long before most people thought of industrial control systems as targets. “Nobody gave it a second thought,” Mayor Joe Soto said. “When it was put in, we didn’t have terrorists.”

The intrusion took all of 10 minutes. The hacker did not cause any damage. Instead, he recorded images of the control system as proof of how easy it was for him to get in.

“I didn’t actually know what the machine was going to control when I started, but I logged in, and well, saw the stuff I took screen shots of,” he said in an e-mail exchange. “I was just amazed.”

So was Soto, after he saw images of the plant’s control panels on the Internet. He and other town officials ordered the gap closed immediately and then considered the implications.

“We’re probably not the only one who is wide open,” Soto said later. “He caught everyone with our pants down.”
Understanding cyberspace is key to defending against digital attacks

By Robert O’Harrow Jr., Published: June 2

Charlie Miller prepared his cyberattack in a bedroom office at his Midwestern suburban home.

Brilliant and boyish-looking, Miller has a PhD in math from the University of Notre Dame and spent five years at the National Security Agency, where he secretly hacked into foreign computer systems for the U.S. government. Now, he was turning his attention to the Apple iPhone.

At just 5 ounces and 4 1/2 inches long, the iPhone is an elegant computing powerhouse. Its microscopic transistors and millions of lines of code enable owners to make calls, send e-mail, take photos, listen to music, play games and conduct business, almost simultaneously. Nearly 200 million iPhones have been sold around the world.

The idea of a former cyberwarrior using his talents to hack a wildly popular consumer device might seem like a lark. But his campaign, aimed at winning a little-known hacker contest last year, points to a paradox of our digital age. The same code that unleashed a communications revolution has also created profound vulnerabilities for societies that depend on code for national security and economic survival.

Miller’s iPhone offensive showed how anything connected to networks these days can be a target.

He began by connecting his computer to another laptop holding the same software used by the iPhone.
Then he typed a command to launch a program that randomly changed data in a file being processed by the software.

The alteration might be as mundane as inserting 58 for F0 in a string of data such as “0F 00 04 F0.” His plan was to constantly launch such random changes, cause the software to crash, then figure out why the substitutions triggered a problem. A software flaw could open a door and let him inside.

“I know I can do it,” Miller, now a cybersecurity consultant, told himself. “I can hack anything.”

After weeks of searching, he found what he was looking for: a “zero day,” a vulnerability in the software that has never been made public and for which there is no known fix.

The door was open, and Miller was about to walk through.

**Holes in the system**

The words “zero day” strike fear in military, intelligence and corporate leaders. The term is used by hackers and security specialists to describe a flaw discovered for the first time by a hacker that can be exploited to break into a system.

In recent years, there has been one stunning revelation after the next about how such unknown vulnerabilities were used to break into systems that were assumed to be secure.

One came in 2009, targeting **Google, Northrop Grumman, Dow Chemical** and hundreds of other firms. Hackers from China took advantage of a flaw in Microsoft’s Internet Explorer browser and used it to penetrate the targeted computer systems. Over several months, the hackers siphoned off oceans of data, including the source code that runs Google’s systems.

Another attack last year took aim at cybersecurity giant RSA, which protects most of the Fortune 500 companies. That vulnerability involved **Microsoft Excel, a spreadsheet program. The outcome was the same: A zero-day exploit enabled hackers to secretly infiltrate RSA’s computers and crack the security it sold. The firm had to pay $66 million in the following months to remediate client problems.**

The most sensational zero-day attack became public in the summer of 2010. It occurred at Iran’s nuclear processing facility in Natanz. Known as **Stuxnet**, the attack involved a computer “worm” — a kind of code designed to move throughout the Internet while replicating itself. Last week, the New York Times reported that President Obama had approved the operation as part of a secret U.S.-Israeli cyberwar campaign against Iran begun under the Bush administration.

Among other things, the worm was built to infect thumb drives. Investigators think that when one of the infected drives was inserted into a computer at the Natanz plant, its code quickly found its target: It made hundreds of centrifuges designed to refine uranium run too fast and self-destruct, while sending signals to monitors that all was well.

To complete its mission, the Stuxnet worm relied on four zero days.

Just days ago, researchers released information about Flame, another cyberattack. It appears to be designed as a massive espionage and surveillance tool, also aimed at Iran, that can steal data and listen in on phone calls.

http://www.washingtonpost.com/investigations/understanding-cyberspace-is-key-to-defen... 11/19/2012
Some researchers believe it exploits zero-day vulnerabilities similar to those in Stuxnet.

The vastness of cyberspace

Miller and his kind are masters of code. At a fundamental level, there is almost nothing simpler than the stuff of their obsessions. There is software, which is written computer language. Computers transform software into machine code, which is simply 0’s and 1’s. Those “binary digits,” or bits, organized in trillions of combinations, serve as both the DNA and digital blood of our modern electronic world.

Bits guide the electrical impulses that tell the world’s computers what to do. They enable the seemingly magical applications that computer and smartphone users take for granted. Bits have also given life to the most dynamic man-made environment on Earth: cyberspace.

Not too long ago, “cyberspace” was pure fiction. The word appeared in “Neuromancer,” a 1984 novel that described a digital realm in which people, properly jacked in, could navigate with their minds. Author William Gibson described it as a “consensual hallucination experienced daily by billions of legitimate operators.”

Now cyberspace is a vital reality that includes billions of people, computers and machines. Almost anything that relies on code and has a link to a network could be a part of cyberspace. That includes smartphones, such as the iPhone and devices running Android, home computers and, of course, the Internet. Growing numbers of other kinds of machines and “smart” devices are also linked in: security cameras, elevators and CT scan machines; global positioning systems and satellites; jet fighters and global banking networks; commuter trains and the computers that control power grids and water systems.

So much of the world’s activity takes place in cyberspace — including military communications and operations — that the Pentagon last year declared it a domain of war.

All of it is shot through with zero days.

“We have built our future upon a capability that we have not learned how to protect,” former CIA director George J. Tenet has said.

Researchers and hackers, the good guys and bad, are racing to understand the fundamental nature of cyberspace. For clues about how to improve security — or to mount better attacks — they have turned to physics, mathematics, economics and even agriculture. Some researchers consider cyberspace akin to an organism, its security analogous to a public health issue.

One of the things they know for sure is that the problem begins with code and involves what “Neuromancer” described as the “unthinkable complexity” of humans and machines interacting online.

“The truth is that the cyber-universe is complex well beyond anyone’s understanding and exhibits behavior that no one predicted, and sometimes can’t even be explained well,” concluded JASON, an independent advisory group in the nation’s top scientists, in a November 2010 report to the Pentagon. “Our current security approaches have had limited success and have become an arms race with our adversaries.”

Hacker life
To picture the scale of cyberspace and the scope of the cybersecurity problem, think of the flow of electronic data around the world as filaments of light. Those virtual threads form a vast, brilliant cocoon around the globe.

The electronic impulses that carry the data move at lightning speed. A round-trip between Washington and Beijing online typically occurs in less than it takes for a major leaguer’s fastball to cross home plate. Blink, and you miss it.

It almost doesn’t matter where hackers work. In the physics governing cyberspace, hackers, terrorists and cyberwarriors can operate virtually next door to regular people browsing the World Wide Web or sending e-mails or phone texts.

Charlie Miller works in suburban St. Louis, in a room that has a small desk, a laptop, a large monitor and power cords that snake across the floor. A wooden bookshelf holds technical manuals alongside his kids’ plastic toys and stuffed animals.

The main clue about what he does for a living is a wall poster for the movie “Hackers.” “Their Crime Is Curiosity,” it says.

The 39-year-old Miller is regarded by some as among the best hackers in the world, but he does not fit the stereotype of an alienated outsider. For starters, he is one of the good guys, a white-hat hacker. He is a security consultant, and he hunts zero days as a hobby. A father of two, trim and balding, he is deceptively modest about his special talents. But his résumé entry about his NSA experience speaks volumes:

“Performed computer network scanning and reconnaissance. Identified weaknesses and vulnerabilities in computer networks. Executed numerous computer network exploitations against foreign targets.”

Apple would not be happy about his plan to attack the iPhone. Like other technology companies, Apple does not want questions about security to taint its products. The company has a well-deserved reputation for developing strong software systems. (Apple officials declined to comment for this article.)

But Miller wasn’t being malicious. He wanted to have fun, prove that it could be done and let the attack serve as a warning about the insecurity of the networked world.

Most of all, he wanted to win a prestigious annual contest where hackers convene to show off the skills that they generally keep to themselves. To win the contest, known as “Pwn2Own,” Miller had to discover a zero day and exploit it. (Pwn is hacker lingo for taking control of a computer.)

If he won, he would receive $15,000, the device he had pwned and a white blazer (modeled on the green jacket worn by winners of the Masters golf tournament). He had won the prize before for hacking Apple products, but it was getting harder.

As he settled into a large black swivel chair in his office, Miller knew he had a challenge on his hands. He did not doubt whether he would find a flaw. He only wondered how bad it would be.

**Cracking the iPhone**

In December 2010, Miller reached out to a friend and security colleague, Dionysus Blazakis.
Blazakis, 30, started hacking in 1994 and has been breaking code ever since. But instead of breaking the law, he decided to become a software developer. He and Miller worked for the same computer security firm in Baltimore, Independent Security Evaluators. He's also a zero-day hunter.

In instant chat messages, the two bantered about the technical details of the iPhone's software. Like hackers everywhere, they wanted to find the easiest route to a vulnerability that would let them take control. Unlike most hackers, they had a deadline: The contest began on March 9, 2011.

"Where do you start? . . . What do you focus on?" Miller recalled asking himself. "The hard part is figuring out the soft part to go after."

Reading through all the software instructions was out of the question. That might have worked two decades ago, when computer systems were simpler and the Web was still a novelty. A desktop computer then might have a million lines of software. Today, the software in a desktop computer could have 80 million lines or more. Finding the zero days by hand would be like searching a beach for a grain of sand of a particular shade of tan.

Miller and Blazakis decided to rely on a hacker technique known as "fuzzing" — inserting random data into applications and trying to force them to crash.

Making systems crash is easier than it might seem. Software programs are miracles of human ingenuity, veritable cathedrals made of letters and digits. But unlike Notre Dame in Paris or the Duomo in Milan — which took lifetimes to build and remain sturdy to this day — digital architecture is constantly evolving and can be made to crumble with the right push at the wrong spot.

Miller attributes that fragility to companies that place sales and novel applications over computer security.

"Companies want to make money," he said. "They don't want to sit around and make their software perfect."

Many of those vulnerabilities are related to errors in code designed to parse, or sort through, data files sent over the Internet. A typical computer has hundreds of parser codes in its operating system. One good example is an image parser. It identifies the information that makes up a digital photo, processes it and then sends the file to the part of the machine designed to display the image.

Hackers will insert corrupted data in the photo's code to disrupt the parser software, cause it to crash and open the way for it to be hijacked.

"If an application has never been fuzzed, any form of fuzzing is likely to find bugs," Microsoft researchers said in a recent paper on the use of fuzzing to improve security.

No human being fuzzing by hand could cause a sufficient number of crashes to routinely allow a hacker to identify a zero day. So Miller and others write programs to do it. Miller's fuzzing program enables him to connect to a variety of computers and keep track of thousands of crashes, including where in the software the crash took place.

"99.999 percent of the time, nothing bad happens," Miller explained. "But I do it a billion times, and it happens enough times it's interesting."
The heart of his program is a function that randomly substitutes data in a targeted software program. He called the 200 lines of code that make up this function his “special sauce.”

To begin his iPhone hack, he took four Apple computers, one a laptop borrowed from his wife, and connected them to another computer holding the iPhone’s software, the entire amalgamation spread over the benchlike desks of his home office. The homey set-up, complete with an overstuffed bookcase crowned by a bowling pin, looked like the lair of a graduate student pursuing a science project.

Miller ran the mini-network 24 hours a day for weeks. One machine served as the quarterback, launching and coordinating the fuzz attacks, tracking the crashes and collecting the details. Before 7 most mornings, he woke up, went into the office, signed into the quarterback computer and checked on the progress, like a kid hoping for snow.

He was on the lookout in particular for failures that involved computer memory management — a serious flaw that could offer the way in.

“The memory manager keeps track of where things are, where new things should go, et cetera,” Miller recalled. “If a program crashes in the memory manager, it means the computer is confused about what things are located where. This is pretty serious, because it means it is in a state where it might be persuaded to think my data is something it thinks is entirely something else.”

For now, most of the crashes were trivial. February was approaching, and time was short. Miller and Blazakis still did not have their zero day.

The hunt for flaws

Zero days have become the stuff of digital legend. In the 1996 science-fiction movie “Independence Day,” characters played by Will Smith and Jeff Goldblum launched a “virus” that took advantage of a zero-day vulnerability, crashed the computer system of an alien mothership and saved the world.

But they have always been more than just science fiction. For decades, hackers and security specialists have known about the existence of zero days. And as software proliferated, along with computers and networks, so have zero days. The researchers who found them often had no incentive to share their finds with the affected companies. Sometimes the researchers simply released the vulnerabilities publicly on the Internet to warn the public at large.

Government agencies that secretly engaged in hacking operations, along with some affected software makers, bought information on zero days from a thriving gray market, according to interviews with hackers and security specialists.

In 2005, a security firm called TippingPoint began offering bounties to researchers. Executives of the Austin-based firm reasoned that they could learn much for their own use while spurring the industry to fix threats by creating a master list. They called their effort the Zero Day Initiative.

Since then, more than 1,600 researchers have been paid for reporting almost 5,000 zero days. Starting at hundreds of dollars, the bounties soar into the tens of thousands. A hacker in Shanghai named Wu Shi has earned close to $300,000 for reporting more than 100 flaws in Web browsers.

The system seemed ideal, except for one thing: The software makers often failed to heed the warnings.
Some vulnerabilities remained for two years or more.

In 2007, TippingPoint, now owned by Hewlett-Packard, decided to underscore the problem by holding a high-profile event. The Pwn2Own contest would require hackers to not only find zero days but to put them into action in what is known as an "exploit" or attack.

Getting closer


"Figuring out what to look at," Miller wrote to his partner, "so we're ready to rock."

They had found it inside the part of the browser software that enables iPhone users to view PowerPoint presentations. It involved portions of the file that stored information about the location and size of shapes, such as a circle, square or triangle that would appear on a page of a presentation.

"Really, it was just bytes in a file. It just happened that it had something to do with a shape. We didn't really care," Miller said later. "As long as it was doing something wrong with the data."

This could be their zero day, but more testing was required to see if they could exploit it.

Both men dived back into the technical details of the iPhone's PowerPoint software. It was hard labor, even for highly skilled hackers. Blazakis stopped shaving and grew a "hacker's beard." He put in 18-hour days as he tried to reverse engineer the PowerPoint application in order to take control of it without causing too much disruption.

Bit by bit, they began mastering the layout of the PowerPoint software. They developed an understanding of it that rivaled those who designed it.

Finally, they found a way to insert their malicious code into the application and take control of a part of the iPhone.

"I think it's under control now," Miller wrote during an instant-message exchange on Jan. 27. "Sweet."

Now they had to complete the exploit by figuring out a way to insert that code into an iPhone and ensuring that they could consistently hijack the device. Unlike the movies, where hackers are portrayed as breaking into computers as if they were cracking into digital safes, successful hacks often require deception and the unwitting complicity of the victim.

On Feb. 3, Miller joked to his friend about their struggle: "Looking for bugs fame money girls glory."

Miller and Blazakis decided to create a way to lure an iPhone user to a bogus Web page. They would set up the page and trick a user into downloading a PowerPoint file. The file would appear normal, but it would contain their malicious code. (Known as "social engineering," it's the same technique used in the Google and RSA attacks.)

With the deadline looming, they began having video conference calls. They linked their computers in cyberspace and worked in tandem. They were a tired but formidable pair, cutting corners on their day jobs as security researchers as they closed in on the elusive exploit.
“The last two days were chaotic,” Blazakis said. “I stayed up most of the night doing this.”

On March 8, Miller flew to the contest, which was part of a security conference in Vancouver, B.C. But they still were not sure of the exploit. They continued fiddling with it right up to the eve of the event, including during Miller’s stopover in Seattle.

Their chance came on March 10. As he sat with judges and other hackers in a narrow conference room set up in the hotel, Miller had lingering fears that the hack still might not work on demand. Under the contest rules, he had just five tries to make it work.

When Miller’s turn arrived, he went behind a long table at one end of the room, where the judges sat with their own computers. Yellow cables snaked through the area (the hackers use cables instead of wireless to prevent other hackers from swiping the zero days in play). Miller connected his old white Apple laptop and looked out at other hackers, spectators and some reporters milling about.

A judge played the role of the unwitting iPhone user. The test phone was placed in an aluminum box to block unwanted wireless signals as an additional measure against any attempted theft of a zero-day exploit by other hackers. Miller told him to browse to the phony Web page holding a PowerPoint presentation that Miller had created. Hidden in the presentation’s data was the malicious code.

The image of the phone’s browser was projected onto a large screen. The judge typed in an address for the Web page, but the presentation never appeared. Instead, the image on the screen jumped back to the home page of the phone.

Miller, sitting with his own computer, knew just what had happened. In that moment, he had gained access to all the names and other information on the phone’s address book. He had found a way to strip privacy protections from a key part of the device.

He nudged one of the judges sitting near him and pointed to his screen, which was displaying the iPhone’s address book. He and Blazakis, who was looking on via a video feed to an iPhone he was holding in Baltimore, had won.

The next day, Miller received an oversize check worth $15,000 and beamed as he put on the white winner’s jacket.

Several weeks later, Apple acknowledged the exploit indirectly when the company issued a “patch.” As a result of the hackers’ work, the flaw they found and exploited was no longer a zero day.

Miller and Blazakis knew that behind the contest’s irreverent fun was a sobering reality.

“We’re smart and have skills and such, but we’re not that extraordinary,” Miller said later. “Imagine if you were a government or a Russian mob or a criminal syndicate and you could get 100 guys like us or 1,000 guys?”
Keeping Watch on the Detectives

DECEMBER 22, 2011

David Cole

One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty
by Simon Chesterman
Oxford University Press, 297 pp., $45.00

Nothing to Hide: The False Tradeoff Between Privacy and Security
by Daniel J. Solove
Yale University Press, 245 pp., $25.00

The Rights of the People: How Our Search for Safety Invades Our Liberties
by David K. Shipler
Knopf, 366 pp., $27.95

In September 2005, federal law enforcement agents in the District of Columbia suspected Antoine Jones, a local nightclub owner, of drug trafficking. Without a
valid warrant, they installed a Global Positioning System (GPS) device on his car, and monitored it around the clock for four weeks. The monitoring led to the discovery of substantial amounts of cocaine. Jones was convicted of conspiracy to distribute the drug, and sentenced to life imprisonment.

The US Court of Appeals for the D.C. Circuit ruled that the GPS monitoring of Jones’s car was a warrantless search in violation of the Fourth Amendment, and reversed his conviction. The Obama administration sought review in the Supreme Court, contending that such monitoring invades no privacy, and therefore requires no warrant, no probable cause, not even any specific suspicion of wrongdoing. On November 8, the Court heard arguments in the appeal; a decision is expected by June.

*United States v. Jones* is the most important privacy case to reach the Supreme Court in years. It requires the Court to decide whether the Fourth Amendment’s safeguards remain meaningful in the digital age, when widely available technological innovations—including GPS devices, cell phones, computer data-mining programs, and the like—make it possible to watch citizens more intimately and comprehensively than was remotely conceivable when the Bill of Rights was adopted.

These devices give the state the Orwellian ability to follow virtually every movement people make and their every keystroke at the computer. If, as the Obama administration would have it, the state can engage in such monitoring without first developing any objective basis for suspicion, privacy may become as “quaint” and “obsolete” as then White House counsel Alberto Gonzales once characterized the Geneva Conventions. As Justice Stephen Breyer observed during the oral argument, the administration’s theory would allow the state to use GPS devices to monitor “twenty-four hours a day the public movement of every citizen of the United States.” Or as Chief Justice John Roberts put it, bringing the point even closer to home, nothing would stop the FBI from using GPS devices to monitor the justices’ own vehicles.

The *Jones* case arises from the ongoing “war on drugs,” which has simultaneously made the United States the uncontested world leader in per capita incarceration, prompted the radical dilution of Fourth Amendment protections, and done little to limit the ready availability of drugs. But the issues *Jones* presents are equally pressing with respect to that other war, the “war on terror,” which continues despite the Obama administration’s jettisoning of the label.
The Fourth Amendment’s core requirement that the state obtain a warrant based on “probable cause” before conducting a search is what protects the privacy of our homes, thoughts, and relationships from prying government surveillance. But it poses a challenge to both anti-drug and anti-terrorism efforts. “Probable cause” is generally defined as …

This article is available to subscribers only.
Please choose from one of the options below to access this article:

- Purchase a trial Online Edition subscription and receive unlimited access for one week to all the content on nybooks.com. $4.99
- Purchase a print subscription (20 issues per year) and also receive online access to all articles published within the last five years. $74.95
- Purchase an Online Edition subscription and receive full access to all articles published by the Review since 1963. $69.00

If you already have one of these subscriptions, please be sure you are logged in to your nybooks.com account. If you subscribe to the print edition, you may also need to link your web site account to your print subscription. Click here to link your account services.
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS: DIGITAL SCANS TO PROTECT THE NATION'S CRITICAL INFRASTRUCTURE AND KEY RESOURCES

Scott J. Glick

Copyright (c) 2012 University of the Pacific, McGeorge School of Law; Scott J. Glick

Introduction

In the twenty-first century, the Internet has revolutionized our ability to communicate, socialize and engage in commerce, and has become an “essential part of daily life of millions of Americans.” While it may have begun as a Department of Defense project to create a computer network that could survive a nuclear war, and in its earliest phases was used as a means of communication between academics, scientific researchers, and the government, today the Internet “is a global network of interconnected communication and information systems.” That is both good news and bad news because the same Internet that connects us to each other and to the world also connects the world to the “nervous system of the country,” including our nation’s critical infrastructure and key resources. Moreover, the Roman Empire may have been able to control the roads that it built to enable its empire to flourish, neither federal nor state governments own all of the “virtual roads” that exist in cyberspace. Indeed, the private sector, rather than the government, owns “most of our critical cyber infrastructure.”

To be sure, the federal government has taken steps to employ computer intrusion and detection technology to protect its own computer networks. The government’s ability to digitally scan private-to-private electronic or wire communications that are transiting the “.com” or “.org” domains for malicious digital codes, however, raises a fundamentally different Fourth Amendment issue than the government’s ability to digitally scan incoming and outgoing communications on the “.gov” or “.mil” domains. If one were to use a criminal investigatory lens, one would conclude that the “Fourth Amendment ordinarily requires a warrant for the collection of the contents of Internet communications.” Under this view, a Title III wiretap order to obtain the contents of those communications in real time must be issued by a “neutral and detached authority” and the order must be based on individualized suspicion. A “foreign intelligence” lens would also generally require a court order.

But what if, instead of seeking evidence of criminal activity or foreign intelligence information, the government used a different lens and employed computer intrusion and detection technology at certain specific digital locations on the Internet primarily for protective purposes? In the physical world, the government can engage in a variety of protective activities, and the Fourth Amendment does not always require the government to have individualized suspicion or obtain a court order. For example, government agents can conduct international border searches, establish sobriety checkpoints, and engage in security screening searches at domestic airports - all within a legal framework that does not require individualized suspicion of criminal activity or a court order. The question then is whether, in the absence of individualized suspicion and a court order, technology that digitally scans Internet communications for malicious digital codes without initially exposing the contents of...
those communications to human review\textsuperscript{18} may be used without running afoul of *100 the Fourth Amendment. Moreover, if there is a reasonable basis to believe that a malicious digital code may be present, an equally important question is what mechanisms can be put in place to ensure that remedial and other actions taken by the government to protect the nation's critical infrastructure and key resources are reasonable and constitutional.

As background for this article, Part I provides an overview of the cybersecurity risks, as identified by various experts, to the nation's critical infrastructure and key resources. Part II then examines the legal frameworks from the physical world that govern international border searches, sobriety and other checkpoints on public highways, searches by narcotics-detection dogs, screening searches at airport security checkpoints, and Terry-stops, as well as the government's authority to quarantine and isolate persons who have communicable diseases. Part III then argues that by using the correct Fourth Amendment lens, these fairly well established legal frameworks from the physical world strongly support the existence of a new cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements. If appropriate legislation is enacted, the cybersecurity exception will enable the government to conduct reasonable and limited digital scans at virtual checkpoints in cyberspace, when the programmatic purpose of those scans is to identify malicious digital codes that may be attacking the nation's critical infrastructure and key resources. Part III therefore proposes that the Congress consider and enact sensible new legislation that will permit the government to conduct these digital scans and take remedial and other actions to protect the nation without running afoul of the Fourth Amendment and existing law.

I. Cybersecurity Risks To The Nation's Critical Infrastructure And Key Resources

In his May 2009 Cyberspace Policy Review, President Barack Obama declared that “cybersecurity risks pose some of the most serious economic and national security challenges of the twenty-first century.”\textsuperscript{19} Two years later, President Obama unveiled a comprehensive cybersecurity legislative proposal to protect the “Nation's critical infrastructure, and the Federal government's own networks and computers.”\textsuperscript{20}

*101 The rationale for comprehensive cybersecurity legislation is clear. The cybersecurity risks\textsuperscript{21} facing the nation’s critical infrastructure and key resources have dramatically increased over the last decade\textsuperscript{22} and are frequently described in ominous tones. For example, during his recent confirmation hearing for Secretary of Defense, then Central Intelligence Agency Director Leon Panetta stated that the “next Pearl Harbor that we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, and our governmental systems.”\textsuperscript{23} Senator Susan M. Collins, Ranking Member of the U.S. Senate's Homeland Security and Governmental Affairs Committee and a cosponsor of the “Cybersecurity Act of 2012,”\textsuperscript{24} has stated that the nation faces the threat of a “cyber 9/11.”\textsuperscript{25} In addition, Senator Jay Rockefeller, Chairman of the U.S. Senate's Committee on Commerce, Science and Technology and cosponsor of the “Cybersecurity Act of 2012,”\textsuperscript{26} has also stated that a “major cyber attack could shut down our Nation's most critical *102 infrastructure: our power grid, telecommunications, [and] financial services . . . .”\textsuperscript{27}

Similarly, former government officials have spoken about the serious cybersecurity risks facing the nation's critical infrastructure and key resources. For example, Michael Chertoff, former Secretary of Homeland Security, has stated that “[n]etwork electronic warfare can cripple or paralyze domestic and civilian systems.”\textsuperscript{28} Richard Clarke, former Cybersecurity Advisor to President Obama, has also warned that foreign intelligence services have penetrated the control systems of the U.S. electric power grid and have left behind “logic bombs” and “trap doors.”\textsuperscript{29}
The primary reason for these concerns is clear. As former Director of National Intelligence Dennis Blair has stated, the "connectivity between information systems, the Internet and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures."\(^{30}\) As a result, we live in a world where a potential cyber attack is not just a criminal issue affecting individuals or businesses, but one which represents a broader economic risk to the nation.\(^{31}\) Today, the "full dimension" of the cybersecurity risks to the nation include "substantial risks to the command and control of important physical assets such as electric power grids, water supply, and other critical infrastructure."\(^{32}\)

Connectivity, however, is not the only cybersecurity challenge facing the nation. Developing and implementing strategic or tactical plans to protect the nation's critical infrastructure and key resources is complex because experts have identified numerous "threat vectors," including "supply chain and vendor access, remote access, proximity access, and insider access."\(^{33}\) The supply chain and vendor access threat results from the fact that the "global economy" enables our nation to "compete and purchase services in an expanded market" which has "substantially increased our vulnerability to adversarial manipulation of our software and hardware."\(^{34}\) By way of contrast, the remote access threat comes from "computer network intrusions or 'hacking.'"\(^{35}\) On the other hand, the proximity access threat refers to the "abilities our adversaries have when they are physically close to our networks but not directly inside them," and the insider threat comes from trusted persons who are given access to computer networks and systems, such as "employees, contractors, and trusted business partners."\(^{36}\)

The concern about insiders, however, does not arise only from malicious actors. There is no security patch for cyber stupidity, and an employee who inserts a virus-laden USB thumb drive into a networked computer may be as much a threat as the employee who intends to do harm.\(^{37}\) Finally, and perhaps the biggest cybersecurity challenge, intrusion detection systems also face what some experts call the "zero day" threat because "malicious actors develop new malware continually," and anti-virus and other intrusion programs "cannot detect and stop malware that no one has seen before."\(^{38}\)

Under the single-party consent exception to Title III,\(^{39}\) the government is able to use intrusion and detection technology to protect the "gov" and "mil" domains.\(^{40}\) The primary legal issue therefore relates to the "con" and other private sector domains. While existing statutes enable employees of communications service providers to monitor their own networks to protect their "property" rights, to perform "mechanical or service quality control checks," and to intercept and disclose the content of electronic communications if it is "necessarily incident to the rendition" of those services,\(^{41}\) the prevailing conventional legal theory is that if the government were to use an intrusion and detection system to monitor "private-to-private communications, it would likely be considered an interception under the electronic surveillance laws, which require a court order."\(^{42}\) As a result, while increased public awareness of cyber threats and better policy choices, including "multiple solutions" to "the attribution problem,"\(^{43}\) will improve the nation's cybersecurity, and while enhanced partnerships between the government and the private sector, as well as economic incentives, will also lead to "best" (as well as "next") cybersecurity practices,\(^{44}\) reexamining conventional legal theories is essential when "computers systems integral to the infrastructure, economy, and defense of the United States are under constant attack by a growing array of adversaries."\(^{45}\) Stated another way, and to paraphrase former Attorney General John Ashcroft, the cybersecurity risks facing the nation require us to think "outside the box" but "inside the Constitution."\(^{46}\)

II. Legal Frameworks from the Physical World
The Fourth Amendment protects against "unreasonable searches and seizures." A "search" within the meaning of the Fourth Amendment takes place whenever the government intrudes upon "an expectation of privacy that society is prepared to consider reasonable."48 This formulation, which *106 flows from the formulation by Justice Harlan in his concurring opinion in Katz v. United States, 49 breaks down into a "two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?"50 Thus, if the government's conduct violates a person's reasonable expectation of privacy, or if the government's conduct involves a trespass or a physical intrusion upon a constitutionally protected "effect" or area, then "the courts will consider the government's conduct to be a "search" within the meaning of the Fourth Amendment. 51 By way of comparison, "seizures" within the meaning of the Fourth Amendment only take place when there has been a "meaningful interference with an individual's possessory interests in the property,"52 or when there has been a "governmental termination of freedom of movement through means intentionally applied."53 As a result, when the government's actions constitute a search or a seizure within the meaning of the Fourth Amendment, they must not be "unreasonable."54

A Fourth Amendment search or seizure that is conducted without judicial authorization is "per se unreasonable under the Fourth Amendment - subject only to a few specifically established and well-delineated exceptions."55 These exceptions include, but are not limited to, consent searches,56 searches of vehicles,57 searches incident to arrest,58 and searches *107 conducted when exigent circumstances exist.59 Nonetheless, even under these exceptions, government searches and seizures are "ordinarily unreasonable in the absence of individualized suspicion of wrongdoing."60

Notwithstanding these cardinal principles and rules,61 there are "limited circumstances" where the lack of individualized suspicion does not prevent the government from conducting a search without a judicial warrant. Indeed, for nearly a half a century, the Supreme Court has carved out "special needs"62 and "administrative search"63 exceptions to the Fourth Amendment; that is, circumstances where the government is able to intrude upon areas which are protected by the Fourth Amendment without regard to whether individualized suspicion exists.64 As detailed below, in the special needs and administrative search cases, courts will examine whether the search furthers a "special need[, beyond the normal need for law enforcement."65 These cases also look at the "programmatic purposes"66 that are motivating the government's conduct to ensure that the government is seeking to protect against a "concrete danger."67 Here, the programmatic *108 purpose behind a digital scan at a virtual checkpoint would be to minimize the risk of catastrophic damage to the nation's critical infrastructure and key resources from a cyberattack, clearly a compelling and "legitimate objective" of the "highest magnitude" that goes "well beyond" ordinary crime control.68

While a compelling governmental need is a necessary prerequisite, alone it is not a sufficient basis to uphold the constitutionality of a special needs or administrative search. The federal courts also consider other factors, and evaluate the reasonableness of the search by weighing the level of the intrusion and the privacy interests at stake.69 As a result, this part of the article will examine the special needs and administrative search cases, as well as other legal frameworks from the physical world, to determine whether, taken together, they support the existence of a cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements.70

A. International Border Searches
In view of the "global" connectivity of the Internet, it is appropriate to examine the legal framework that governs searches and seizures at the nation's international border. The earliest case in which the Supreme Court commented on international border searches was Boyd v. United States. There, the Court noted that searches at the international border were first authorized by the same Congress that authorized the Bill of Rights and that the "members of that body did not regard searches and seizures of this kind as 'unreasonable,' and [did not consider them to be] embraced within the *109 prohibition of the [Fourth] Amendment." Nearly 40 years later, the Court further commented on such searches for protective purposes. In Carroll v. United States, the Court stated that a traveler may be stopped when he crosses "an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings and effects which may be lawfully brought in." Thereafter, in a series of cases, the Court repeatedly upheld international border searches as part of the government's "longstanding right . . . to protect itself by stopping and examining persons and property crossing into this country." More recently, in City of Indianapolis v. Edmond, although it invalidated a drug checkpoint, the Supreme Court emphasized that its holding did "nothing to alter the constitutional status of . . . border checkpoints," which are grounded in "considerations specifically related to the need to police the border."

The international border search doctrine applies whenever a person or goods enter the United States, irrespective of whether it is on land from an adjacent country, at a place where a ship docks, or the location where a flight arriving from a foreign nation lands for the first time, even if that location is in the interior of the country, because that arrival point constitutes the "functional equivalent" of the international border. Moreover, the permissible scope of such a border search is quite extensive, and the federal courts have upheld searches of baggage, goods, automobiles, persons, and personal items and papers, including computers and electronic media.

The legal principles that flow from an analysis of the international border search cases are clear: searches at the international border or its functional equivalent may be conducted by the government without a warrant and without individualized suspicion. Any "person or thing coming into the United States is subject to search by that fact alone, whether or not there is any suspicion of illegality directed toward the particular person or thing to be searched." As a result, the sovereign's right to protect itself at the digital international border should be at least as coextensive as its right to protect itself in the physical world. Although there may not be a specific geographic boundary to the digital international border, electronic (or wire) communications in cyberspace which originate outside the United States clearly cross the "functional equivalent" of the international border at specific "routers," "switches," or other locations in the United States. While a regulatory scheme that classifies certain malicious digital codes as contraband may be needed, that does not undermine the constitutionality of the government's use of technology to scan for malicious digital codes at the digital international border. The cybersecurity risks to the nation's critical infrastructure and key resources from these codes are "particularly acute" to justify such a protective action by the government. Moreover, if government agents can conduct further searches of a letter at the international border in the physical world when they have a reasonable basis to believe that contraband may be present, they should be able to conduct further searches of electronic communications entering the United States at the digital international border when there is a reasonable basis to believe that a malicious digital code may be present.

B. Sobriety and Other Checkpoints

Conducting digital scans of electronic communications entering the United States from abroad, however, will not provide a doctrinal basis for protecting against malicious digital codes that originate, or appear to originate, inside the United States. The legal framework that governs sobriety checkpoints on the nation's public highways, however, does have application to a
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....

legal framework that can be constructed to govern domestic virtual checkpoints. For example, in Michigan Department of State Police v. Sitz, 91 the Michigan State Police had established sobriety checkpoints at a number of selected sites along state roads in accordance with specific procedures. 92 All vehicles passing through the checkpoints were stopped by the police, and if signs of intoxication were observed, the driver would be directed to a location out of the traffic flow where the police would conduct further sobriety tests. 93 The protective purpose behind the sobriety checkpoints was clear: they were designed primarily to ensure highway safety and eliminate an “immediate, vehicle-bound threat to life and limb.”94

A protective purpose alone, however, was not the only factor that led the Court to conclude that the sobriety checkpoints were constitutional. Indeed, at least three factors were considered essential to the validity of the sobriety checkpoints in Sitz: (1) the State’s “interest” in preventing drunken driving; (2) the extent to which the system could “reasonably be said to advance that interest”; and (3) the “degree of intrusion on individual motorists who [were] briefly stopped.” 95 Since the level of intrusion was minimal96 and the program was reasonably effective, as compared to *112 traditional law enforcement techniques, 97 given the “magnitude of the drunken driving problem” 98 and the state’s interest in “eradicating” 99 that problem, the program was not unconstitutional.100

The Supreme Court has also upheld the use of fixed immigration checkpoints without individualized suspicion. 101 Immigration checkpoint stops are “reasonable” under the Fourth Amendment because the state’s interest in detecting the presence of illegal aliens outweighs the limited intrusion on an individual’s privacy that is caused by the checkpoints. 102 As was the case with sobriety checkpoints, the effectiveness of the fixed immigration checkpoint in United States v. Martinez-Fuerte 103 was a critical aspect of its reasonableness. There, the record established a “rather complete picture of the effectiveness of the . . . checkpoint.”104

By way of contrast, in Delaware v. Prouse, 105 the Supreme Court disapproved of random stops made by Delaware Highway Patrol officers to apprehend unlicensed drivers and unsafe vehicles, since there was no empirical evidence that such stops would effectively promote roadway *113 safety. 106 Indeed, the Court stated that “common sense” indicated that the “percentage of all drivers on the road who were driving without a license was very small and that the number of licensed drivers who will be stopped in order to find one unlicensed operator will be large indeed.”107

In addition to the effectiveness requirement, another key aspect of the Supreme Court’s endorsement of fixed checkpoints is that they must be carried out pursuant to a “plan embodying explicit, neutral limitations on the conduct of individual officers.” 108 The officer’s “discretion” at the checkpoint was, therefore, one of the primary factors that led to the condemnation of the roving checkpoints for aliens in Almeida-Sanchez v. United States. 109 On the other hand, the Supreme Court upheld the use of the fixed immigration checkpoints in United States v. Martinez-Fuerte because they involved “less discretionary enforcement activity,” were conducted in a “regularized manner,” and reassured law-abiding motorists that the stops were “duly authorized” and served the “public interest.” 110 Finally, the locations of the checkpoints were not selected “by officers in the field, but by officials responsible for making overall decisions as to the most effective allocation of limited enforcement resources.”111

One aspect of the sobriety and immigration checkpoint cases that should be further considered in regard to their application to virtual checkpoints in cyberspace, however, is the public nature of the checkpoints, as well as the public notice that accompanies them. Generally speaking, citizens are notified of the existence and location of these checkpoints and are able to observe the manner in which the checkpoints are administered. 112 While the specific persons who are stopped at such checkpoints may
not be personally aware of the existence of the checkpoints until they arrive at them, the public nature of the checkpoints has been a factor that the Supreme Court has noted.\footnote{113}

On the other hand, this factor should not be dispositive of the constitutionality of a virtual checkpoint in cyberspace. Indeed, the virtual checkpoints on the nation's information superhighway that are the subject of this article would only be established after extensive public debate, and only after congressional approval. In such circumstances, it is possible to accommodate public and private interests, and to properly cabin the scope of the government's conduct. If the virtual checkpoints in cyberspace involve minimal intrusion, are reasonably effective, and are administered in a regularized manner that limits the discretion of those administering them,\footnote{114} and if their programmatic purpose is to minimize the cybersecurity risks to the nation's critical infrastructure and key resources and not ordinary crime control,\footnote{115} then they can be constitutional.

C. Searches by Narcotics-Detection Dogs

Cases that concern searches by narcotics-detection dogs also provide an important analytical framework for determining whether digital scans that initially do not involve human review implicate protected Fourth Amendment interests. These cases are sometimes referred to as “binary” search cases because narcotics-detection dogs provide only a “positive or negative response” as to the presence of illegal narcotics.\footnote{116} Two major Supreme Court cases have addressed the relationship between the Fourth Amendment and narcotics-detection dogs: Illinois v. Caballes\footnote{117} and United States v. Place.\footnote{118} In Caballes, an Illinois State Trooper stopped Caballes for speeding on an interstate highway, and another trooper responded to the scene.\footnote{119} While the first trooper was in the process of writing a traffic-related warning ticket, the second trooper accompanied his dog around Caballes’ car, and when the “dog alerted” near the trunk, the resulting search led to the discovery of marijuana.\footnote{120} After concluding that the initial stop was lawful, the Supreme Court went on to analyze whether the dog sniff “unreasonably infringe[d] interests protected by the Constitution.”\footnote{121} The Court concluded that a dog sniff conducted during a lawful traffic stop “does not violate the Fourth Amendment” because it “reveals no information other than the location of a substance that no individual has any right to possess.”\footnote{122} Thus, the non-human, binary intrusion did “not rise to the level of a constitutionally cognizable infringement.”\footnote{123}

The majority in Caballes found support for its decision in the Court's 1983 decision in United States v. Place.\footnote{124} Place had engaged in suspicious behavior as he waited in a ticket line at the Miami International Airport and after he arrived in New York. When Place refused to consent to a search of his luggage, the agents in New York took his bags and subjected them to a “sniff test” by a trained narcotics-detection dog. The dog reacted positively, which led to a search warrant and the discovery of cocaine.\footnote{125} Writing for the majority, Justice Sandra Day O'Connor stated that “given the enforcement problems associated with the detection of narcotics trafficking and the minimal intrusion that a properly limited detention [of personal luggage] would entail, the Fourth Amendment does not prohibit such a detention.”\footnote{126} The Court noted that the use of the narcotics-detection dog was sui generis since the court was aware of “no other investigative technique that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure;”\footnote{127} that is, the canine sniff only revealed the “presence or absence of narcotics, a contraband item.”\footnote{128} Thus, the Court concluded that a “well-trained narcotics detection dog . . . does not expose noncontraband items that otherwise would remain hidden from public view.”\footnote{129} Although the seizure in Place exceeded the “bounds of a permissible investigative detention of the luggage,”\footnote{130} the Court stated that the dog sniff of Place's personal luggage at the airport “did not constitute a ‘search’ within the meaning of the Fourth Amendment.”\footnote{131}
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....

Although it is not a dog-sniff case, *Kyllo v. United States* must be considered in regard to the issue of whether digital scans at virtual checkpoints that initially involve no human review would run afoul of the Fourth Amendment. In *Kyllo*, government agents had used a thermal-imaging detection device to measure the temperature inside of the defendant's garage while they were sitting in a car parked on a public street. The purpose of the device was to detect the cultivation of marijuana. When the device showed that the garage was atypically warm, the agents suspected that *Kyllo* was using it as a marijuana greenhouse. In finding that the use of the device required a warrant, the Supreme Court noted the fact that the search took place in a home, a location where Fourth Amendment protection from the government has historically been the greatest, as well as the fact that the search was not strictly binary in nature. Indeed, writing for the majority, Justice Antonin Scalia noted that the thermal-imaging detection device was also capable of detecting lawful activity, such as "at what hour each night the lady of the house takes her daily sauna and bath." *136*

*117* Some commentators see "tension between the *Kyllo* rule and the logic permitting suspicionless dog sniffs." Others stress that it is critical to "unlink the seizure question from the search question," noting that "if the absence of physical intrusion is seen as a critical component of the search evaluation, then new technologies (and many existing technologies) that produce nonbinary results could conceivably be accepted merely because they are completely noninvasive." Taken together, however, Caballes, Place, and *Kyllo* provide important touchstones that limit the scope of a cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements. First, to the extent that the government may be examining "metadata," which includes Internet Protocol addresses and other non-content information, it is fairly well-settled that metadata does not receive the same level of privacy protection that is afforded to the contents of electronic (or wire) communications. Second, under the approach discussed in this article, the digital scans of the contents of such communications would initially involve no human review and would only be looking for malicious digital "signatures." Finally, such scans would be binary, and further analysis would only take place if there was a reasonable basis to believe that a malicious digital code may be present.

Under these circumstances, reasonable and limited digital scans at virtual checkpoints in cyberspace would be "justified at their inception" and would not unreasonably intrude upon protected Fourth Amendment interests. While legislative exceptions may be needed for certain persons, such as individuals designing computer intrusion and detection technology, that does not detract from the support that these cases provide to, and how they cabin, a cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements.

*118* D. Screening Searches at Airport Security Checkpoints

Screening searches that are conducted at airport security checkpoints also provide important limitations on the scope of a cybersecurity exception. Airport screening searches have been upheld because they are "conducted as part of a general regulatory scheme in furtherance of an administrative purpose; namely, to prevent the carrying of weapons or explosives aboard aircrafts, and thereby to prevent hijackings." Indeed, at the present time, "all luggage that goes onto a plane [may be screened] to ensure that it does not contain any explosive devices or other items that would threaten the safety of the plane." As the Ninth Circuit has noted, the "essential purpose of the scheme is not to detect weapons or explosives or to apprehend those who carry them, but to deter persons carrying such material from seeking to board at all." As long as the "programmatic purpose" motivating the search is not "a criminal investigatory purpose," it is "justified under an administrative search rationale."
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS: ..., 6 J. Nat'l Security L....

To meet the Fourth Amendment's reasonableness test, airport security screening searches must be "limited to searches for guns or explosives, and ... no more burdensome than necessary to achieve that objective."\textsuperscript{149} The federal courts have noted that airline passengers choose to fly on airplanes, and have been notified of the fact that they and their possessions will be subjected to a search for weapons and explosives.\textsuperscript{150} As a result, the *119 screening searches at airport security checkpoints do not require individualized suspicion to be constitutional, despite the fact they could "lead to discovery of contraband and apprehension of law violators."\textsuperscript{151}

Of course, when all passengers are randomly searched,\textsuperscript{152} the decision to search is not subject to the unfettered discretion of the officer in the field. All persons passing through airport security checkpoints are subjected to searches through "established procedures, and those conducting the searches play no part in determining who will choose to include themselves within the group of persons to be screened."\textsuperscript{153} Moreover, because screening searches at airport security checkpoints are only as intrusive as necessary to accomplish their non-law enforcement, protective purpose, the searches are reasonable.\textsuperscript{154} As a result, although airport security checkpoints may not be a perfect analog for virtual checkpoints in cyberspace, they nonetheless inform the scope of a cybersecurity exception to the Fourth Amendment; that is, the initial digital scans for malicious digital codes should be conducted through "established procedures" and should be no more intrusive than is necessary "in the light of the current technology."\textsuperscript{155}

E. Terry Stops z While the "stop and frisk" cases do not fall into the "administrative search" or the "special needs" category of cases, Terry v. Ohio\textsuperscript{156} and its progeny provide an important additional analytical framework to evaluate protective actions that the government should be able to take in cyberspace. The facts in Terry are fairly straightforward. Two men were acting *120 suspiciously on a street corner in downtown Cleveland and talking with a third man, and the police concluded that they were "casing" a store in preparation for an armed robbery.\textsuperscript{157} The officer confronted the men, identified himself, and began to question them. One of the men mumbled something and the officer then spun Terry around and began a pat down. After feeling the outline of a gun, the officer removed the weapon. A pat down of the second man also revealed a concealed weapon.\textsuperscript{158}

When the case reached the Supreme Court, the question was "whether it is always unreasonable for a policeman to seize a person and subject him to a limited search for weapons unless there is probable cause for an arrest."\textsuperscript{159} After "balancing the need to search against the invasion which the search entails," the Court answered the question in the negative, and concluded that law enforcement officers are only required to establish "reasonable suspicion" to justify a brief detention and protective pat down of the outer clothing for weapons.\textsuperscript{160} The Supreme Court then articulated the reasonable suspicion standard, holding that it exists when a policeman can point to "specific and articulable facts which, taken together with rational inferences from those facts," lead the officer "reasonably to conclude in light of his experience that criminal activity may be afoot."\textsuperscript{161}

If a digital scan at a virtual checkpoint in cyberspace leads computer intrusion and detection technology to a reasonable belief that a malicious digital code may be present in an electronic (or wire) communication, then Terry's reasonable suspicion standard and the compelling governmental interest to prevent such a code from harming the nation's critical infrastructure and key resources should permit the government to conduct a cyber-Terry stop and temporarily "detain" the communication for further analysis. Such "detention" and further analysis of the communication should last, however, "no longer than is necessary to effectuate the purpose of the stop."\textsuperscript{162} Thus, the scope of any cyber-Terry stop should be "strictly tied to and justified by the circumstances which rendered its initiation permissible."\textsuperscript{163}
**VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS: ..., 6 J. Nat'l Security L....**

*121 F. The Government's Quarantine Authority*

The legal framework which governs the government's quarantine and isolation authority with respect to communicable diseases that pose a risk to public health has direct application to the legal framework that should govern the government's ability to protect the nation from malicious digital codes that pose a risk to critical infrastructure and key resources. First, it is clear that the federal government's quarantine authority is at its "zenith at the international border." Indeed, the Department of Homeland Security has the authority to prevent the admission into the United States of any alien "who is determined (in accordance with regulations prescribed by the Secretary of Health and Human Services) to have a communicable disease of public health significance." Moreover, such aliens may be temporarily detained at ports of entry for the purpose of determining whether they are inadmissible by virtue of having a communicable disease of "public health significance."  

The ability to quarantine persons travelling domestically within the United States is primarily based upon the "police power" of a state. The Supreme Court has recognized for more than a century that a state has the power to enact "reasonable regulations" to detain and quarantine individuals who pose a threat to "the public health and the public safety." The federal government, however, also has some domestic quarantine authority. For example, the Surgeon General, with the approval of the Secretary of Health and Human Services, has the authority to make and enforce quarantine regulations that are "necessary to prevent the introduction, transmission, or spread of communicable diseases." Although such diseases must be identified by the President, pursuant to a number of executive orders, several communicable diseases that authorize the quarantine of individuals have been identified. Federal quarantine regulations also authorize the apprehension and examination of "any individual reasonably believed to be infected with a communicable disease in a qualifying stage," if the individual is "moving or about to move from a State to another State," or is "a probable source of infection to individuals who, while infected with such diseases in a qualifying stage, will be moving from a State to another State."  

Other statutes and regulations also provide authority to quarantine individuals and take remedial actions. For example, the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 provides the federal government with the ability to engage in "removal" and "remedial" actions to prevent the spread of "hazardous" substances. Such actions include those that "may be necessary to prevent, minimize, or mitigate damage to the public health or welfare or to the environment." The statute also provides that the President may, "after notice to the affected State," take other action including, but not limited to, issuing such orders as may be necessary to protect public health and welfare and the environment.  

The federal government also has the authority to assist state authorities in enforcing a state's quarantine. Indeed, a quarantine may be enforced where it "can be demonstrated that unlimited travel to the area would directly and materially interfere with the safety and welfare of the area or the Nation as a whole." However, a state's quarantine law must not "unreasonably burden or restrict" a person's constitutional right to travel. Thus, the individual must actually pose a risk to public health, and the quarantine may not be imposed in a manner that deprives an individual of his constitutional rights to equal protection and due process. Quarantines must therefore be conducted in accordance with an individual's substantive and procedural due process rights, and in the least restrictive manner as reasonably possible under the circumstances.  

Based on the foregoing, it is clear that the legal framework that governs the government's ability to take remedial actions against persons who pose a health risk as a result of a communicable disease in the physical world informs the legal framework that can be constructed to enable the government to take remedial actions against malicious digital codes in cyberspace. Among
other things, the government's actions in cyberspace should be necessary, the least restrictive as reasonably possible under the circumstances and in light of existing technology, and imposed in a reasonably effective manner to ensure equal protection and due process. While it may be necessary for executive orders and a regulatory scheme to be promulgated, that does not undermine the constitutional support that exists for a legal regime that will enable the government to protect the "safety and welfare" of the nation's critical infrastructure and key resources from malicious digital codes.  

III. Lessons From the Physical World and Proposed Legislation

Some courts and commentators have searched for the "right" analogy to mediate new technology and old rules. Finding such analogies, however, can prove to be illusive because physical world analogies frequently break down in cyberspace when they are scrutinized closely. Others have stated that "new technologies should lead us to look more closely at just what values the Constitution seeks to preserve." While both of these approaches are important, as the foregoing discussion demonstrates, applying the Fourth Amendment correctly to new technologies is also dependent upon the use of the appropriate lens (or framework). Indeed, even if one could find the right analogy and used a values-based approach, one would nonetheless reach an erroneous result if one did not focus on the issues with the correct Fourth Amendment lens. The "lens" method of legal analysis is based upon the premise that one has a better chance of arriving at the correct result only if one begins the *125 analysis with the correct lens. While adherence to underlying values is essential and while policy choices may alter results, if one begins the analysis with the wrong lens, there is a greater chance that when doctrinal principles and values are applied, one will reach erroneous conclusions. Here, it is a protective lens, as opposed to a criminal, intelligence, or military lens, that strongly supports the existence of a cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements.

This cybersecurity exception, however, is a limited one and is appropriately informed by the doctrinal limitations of the special needs and administrative search cases, as well as by the other legal frameworks from the physical world discussed above. While individual aspects of these legal frameworks may not map perfectly to cyberspace, when viewed together, they inexorably lead to the conclusion that reasonable and limited digital scans at virtual checkpoints in cyberspace can be constitutional - notwithstanding the lack of individualized suspicion or a court order - because the programmatic purpose of those scans is to identify malicious digital codes that may be attacking the nation's critical infrastructure and key resources. Moreover, because these digital scans are focused only on identifying the presence or absence of malicious digital codes, there is minimal risk of unwarranted invasions of privacy, particularly as compared to physical searches by law enforcement officers at international borders, sobriety checkpoints, airports, or even in subway stations. Thus, computer intrusion and detection technology that is binary and does not initially expose the contents of electronic (or wire) communications to human review can be a constitutional and effective means to protect the nation's critical infrastructure and key resources.

Addressing the constitutional question, however, does not end the inquiry. Unless a specific statutory exception exists, Title III makes it unlawful to "intentionally intercept" any "wire . . . or electronic communication." While the "prior consent" exception is enumerated in *126 the statute, and while an Internet service provider may intercept Internet communications to protect its property, neither of these statutory exceptions is sufficiently broad to encompass all of the virtual points in cyberspace where the government can and should be detecting the presence of malicious digital codes that may be attacking critical infrastructure and key resources.

As a result, while the foregoing discussion demonstrates that fairly well-established Fourth Amendment doctrines from the physical world provide a solid constitutional foundation for reasonable and limited digital scans for malicious codes at virtual checkpoints in cyberspace, an explicit statutory cybersecurity exception is needed in Title III. Such an exception could read along the following lines:
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....

Notwithstanding any other law, it shall not be unlawful for an officer, employee, or agent of the United States, or of any State, in the normal course of his official duty, to conduct reasonable and limited digital scans of electronic or wire communications in order to identify, quarantine, or isolate any malicious digital code that may be attacking, has attacked, or is about to attack the critical infrastructure or key resources of the United States or of any State.

In view of the important policy choices that are at stake, however, any legislation should be guided by the principles discussed below. Indeed, a free and open Internet is essential to the continued economic vitality of our nation. Thus, in seeking to create a legal framework for protective actions in cyberspace, the government must ensure that it does not unreasonably infringe upon cherished constitutional freedoms and values. As one former Department of Justice official has noted, expanding a computer intrusion and detection system to the public Internet may very well cause the "Internet culture [to] rise up in revolt." While reasonable people may disagree about whether this overstates the case, any new cybersecurity legal framework must be mindful of the "privacy rights and civil liberties [that are] guaranteed by the Constitution and law." Public debate is therefore critical, particularly in view of the policy choices that are available to the nation's lawmakers, and "[c]oncrete mechanisms to protect privacy and to ensure that the government's search is minimally intrusive and reasonably efficacious" are essential.

New cybersecurity legislation, executive orders, and regulations that authorize the government to use reasonable and limited digital scans at virtual checkpoints in cyberspace, and to take remedial and other actions should therefore be informed by the following:

A. Digital scans at virtual checkpoints in cyberspace should be administered in a regularized, fair and reasonable fashion pursuant to established regulations and procedures which do not permit arbitrary or capricious scanning that is unrelated to the protection of critical infrastructure and key resources;

B. Digital scans should be conducted in the least intrusive means necessary to accomplish their purpose in light of existing technology; that is, they should not initially expose the contents of the communications to human review, and they should be binary and determine whether or not there is a reasonable basis to believe that a malicious digital code may be present;

C. Mechanisms should be put in place to ensure that regular government and Congressional oversight exists; that is, the executive branch and the legislative branch should ensure that the digital scans continue to be necessary in light of the cybersecurity risks, and that they are reasonably accurate and effective at identifying malicious digital codes that have attacked, may be attacking, or are about to attack, critical infrastructure and key resources;

D. If a digital scan leads to a reasonable belief that a malicious digital code may be present, then a cyber-Terry stop should take place which enables the government to use the least intrusive means reasonably available, under the circumstances and in light of existing technology, to verify or dispel its belief that a malicious digital code may be present; and

E. Cybersecurity quarantine and related authorities should be promulgated to enable the government to take reasonably effective remedial and other actions against malicious digital codes. Any regulatory scheme, however, should be as minimally restrictive as reasonably possible, under the circumstances and in light of existing technology, to ensure equal protection and due process.

Conclusion
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:.... 6 J. Nat'l Security L....

The cybersecurity risks to the nation are significant and increasing every day, and unless those risks are minimized, there could be serious and devastating consequences to the nation's critical infrastructure and key resources. As a result, at this moment in time, the nation needs to answer two key "foundational" questions; namely, "what technical tools are the American people comfortable having the government deploy, and what level of government involvement and interaction with the private sector will the people allow." While a sound legal basis exists for the government to use computer intrusion and detection technology to protect its own networks without the need for a court order or individualized suspicion, and while there are several cybersecurity policies that can and should be implemented, new thinking is required if the nation is going to be able to minimize the cybersecurity risks to our critical infrastructure and key resources, which are primarily owned by the private sector.

When viewed through a protective Fourth Amendment lens, fairly well-established legal frameworks from the physical world can provide a sound doctrinal basis for finding a new cybersecurity exception to the Fourth Amendment's individualized suspicion and warrant requirements. While certain aspects of these legal frameworks may not map perfectly to cyberspace, when viewed together, they strongly support a cybersecurity exception that enables the government to conduct reasonable and limited digital scans at virtual checkpoints in cyberspace to minimize the risks posed by malicious digital codes that may be attacking the nation's critical infrastructure and key resources. Congress should therefore consider and enact sensible new legislation that will allow digital scans at virtual checkpoints and cyber-Terry stops to take place within the constitutional framework that has enabled this nation to prosper.

Footnotes

1 Senior Counsel, National Security Division, U.S. Department of Justice. This article has been reviewed for publication by the Justice Department in accordance with 28 C.F.R. §17.18. The views expressed in this article are solely those of the author and do not necessarily reflect the views of the Justice Department. The author wishes to thank Stephen Dycus, Stephen Vladeck, David Rosenberg, Mark Eckenwiler, Jordan Strauss, Joshua Geltzer, and Dena Roth for their review and comments on an earlier draft of this article.


3 Todd M. Hinnen, The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet, 5 Colum. Sci. & Tech. L. Rev. 5, 8 (2004).


5 The definitions of "critical infrastructure" and "key resources" have been described as "evolutionary" and "ambiguous." John Motzef and Paul Parfomak, Critical Infrastructure and Key Assets: Definition and Identification (Cong. Res. Service RL 32631), Oct. 1, 2004, at 2. At the present time, 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." Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, §1016(e), Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified at 42 U.S.C. §195C(e) (2006)). In addition, the term "key resources" means "publicly or privately controlled resources essential to the minimal operations of the economy and government." Homeland Security Act of 2002, §2(9), Pub. L. No. 107-296, 116 Stat. 2135 (2002) (codified at 6 U.S.C. §101(10) (2006)).
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....

As Federal Bureau of Investigation Director Robert Mueller aptly noted during a cybersecurity speech he gave at Penn State University in 2007, while the Roman Empire was able to flourish for hundreds of years, in the end it was overrun by millions of invaders who used the same roads that had originally been built to spread Roman civilization and influence. See Steven R. Chabinsky, Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line, 4 J. Nat'l Security L. & Pol'y 27, 29 (2010).

Arguably, the roads in cyberspace are more physical than virtual because the basic architecture of the network - including the computers, wires, cables, servers, routers and switches that allow it to function - physically exist at various locations around the country. See Cybersecurity Hearing, supra note 4 (testimony of Associate Dep. Atty General James A. Baker) (the “Internet is a physical thing, and it exists in different places” in the physical world); see also Barbara van Schewick, Internet Architecture and Innovation 84 (2010) (the Internet “connects different physical networks”).


As used in this article, the term “malicious digital codes” refers to any kind of computer virus, worm, bot-net, spyware, malware, Trojan horse, network exploitation or infiltration code, or any other malicious digital or computer codes that enable malicious actors to inflict harm or obtain control of the computers, networks and devices that control and operate the nation's critical infrastructure and key resources. See OLC Legal Issues Memorandum, supra note 9 at 3 n.3; Nat'l Institute of Justice, Investigations Involving the Internet and Computer Networks 55 (2007), available at http://www.ncjrs.gov/pdfiles1/nij/210798.pdf.

The Fourth Amendment reads: “The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV.

Kerr, supra note 1, at 1039.


For a discussion of some of the government's military authorities in cyberspace, which are beyond the scope of this article, see Herbert S. Lin, Offensive Cyber Operations and the Use of Force, 4 J. Nat'l Security L. & Pol'y 63 (2010); David E. Graham, Cyber Threats and the Law of War, 4 J. Nat'l Security L. & Pol'y 87 (2010).

See infra Section II.

See Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 535 (2005) (a search is best described as the process by which “data is exposed to human observation”).
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:... 6 J. Nat'l Security L....


21 While "risk" and "threat" are often used interchangeably, experts have cautioned against exclusively looking at threats to assess cybersecurity risks. Instead, they recommend use of the "classic risk formula." See Chabinsky, supra note 6, at 35 ("Risk = Threat x Vulnerability x Consequence.").

22 Cybersecurity Hearing, supra note 4, at 2 (statement of Associate Dep. Att'y Gen. James A. Baker), available at http://www.judiciary.senate.gov/pdfs/11-06-21%20Joint%20C20%20Stateemen%20en%20James%20Baker,%20Greg%20Schaefer,%20and%20Schwartz.pdf. See OLC Legal Issues Memorandum, supra note 9, at 2 ("Over the past several years, Federal Systems have been subject to sophisticated and well-coordinated computer network intrusions and exploitations on an unprecedented scale. The Intelligence Community has determined that these malicious network activities pose a grave threat to national security."); see also John Rollins & Anna Henning, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations (Cong. Res. Service R40427) Mar. 10, 2009, at 2 ("Threats to the U.S. cyber and telecommunications infrastructure are constantly increasing and evolving as are the entities that show interest in using a cyber-based capability to harm the nation's security interests." (footnotes omitted)).


28 Michael Chertoff, Foreword, Cybersecurity Symposium: National Leadership, Individual Responsibility, 4 J. Nat'l Security L. & Pol'y 1, 1 (2010); see also Cyber Security: Responding to the Threat of Cyber Crime and Terrorism: Hearing Before the Subcommittee on Crime and Terrorism of the S. Comm. on the Judiciary, 112th Cong. 5 (statement of Stewart Baker, former Ass't Sec'y for Policy, Dep't of Homeland Security), available at http://judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862735da16a99598&wit_id=e655f9e2809e5476862735da16a9959-2-2 (warning that the tools the "stuxnet" virus deployed could "just as easily be used to bring down the power grid for a city or a region").


Annual Threat Assessment of the Intelligence Community: Hearing Before the S. Select Comm. on Intelligence, 111th Cong. 38 (2009) (testimony of Director of National Intelligence Dennis Blair), available at http://www.dni.gov/testimonies/26090212_testimony.pdf (arguing that a successful cyber attack could “severely impact the national economy”); see also Burstin, supra note 4, at 168 (“[M]odern attacks threaten to target infrastructure that is integral to the economy, national defense, and daily life.”).

Chabinsky, supra note 6, at 28 n. 3 (emphasis supplied); see also Dep’t of Homeland Sec., Primer Control Systems Cyber Security Framework and Technical Metrics (2009), available at http://www.us-cert.gov/control_systems/pdf/Metrics_primer&uscore_v9_7-13-09_FINAL.pdf (“Electronic control systems that operate much of the Nation’s critical infrastructure are increasingly connected to public networks, including the Internet ... and are at greater risk than before from externally initiated cyber attacks.”); Goldsmith, supra note 27, at 1 (“[O]ur energy supply, our means of transportation, and our military defenses are dependent on vast, interconnected computer and telecommunications networks ...”); Dominic Basulto, Digital Deterrents: Preventing a Pearl Harbor of Cyberspace, Wash. Post (Oct. 17, 2011), http://www.washingtonpost.com/blogs/innovations/post/digital-deterrents-preventing-a-pearl-harbor-of-cyberspace/2010/12/20/gIQASN6YoL_blog.html (“The Internet has become the back door and front door to controlling nearly every aspect of our national infrastructure.”).

Chabinsky, supra note 5, at 32.


Chabinsky, supra note 6, at 34.


See Frank L. Greitzer et al., Combating the Insider Cyber Threat, IEEE Security & Privacy, Jan.-Feb. 2008, at 61, 61, available at www.cert.org/archive/pdf/combatsthr0408.pdf (“The insider threat is manifested when human behavior departs from compliance with established policies, regardless of whether it results from malice or a disregard for security policies.”).

Cybersecurity Hearing, supra note 4, at 4; see also Lin, supra note 16, at 65 n.7 (“The term [zero day attack] refers to the fact that the vulnerability has been known to the defender for zero days.”).

See 18 U.S.C. §2511(2)(c) (2006) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire ... or electronic communication, where ... one of the parties to the communication has given prior consent to such interception.").

The Office of Legal Counsel of the U.S. Department of Justice has opined that when “log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system,” the Einstein 2 intrusion and detection technology employed by executive branch departments and agencies is lawful. Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch, Memorandum Opinion for an Associate Deputy Attorney General, Office of Legal Counsel 1 (Aug. 14, 2009), available at http://www.justice.gov/olc/2009/legality-of-e2.pdf; see also OLC Legal Issues Memorandum, supra note 9.
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....


Gregory T. Nojeim, Cybersecurity and Freedom on the Internet, 4 J. Nat'l Security L. & Pol'y 119, 124 (2010). By way of contrast, “metadata” information, which includes the “addressing information for e-mails, IP addresses of visited Web sites, routing information that tracks a communication’s path on the Internet, and possible traffic volume information... does not implicate the Fourth Amendment.” Goldsmith, supra note 27, at 11.

See 156 Cong. Rec. S7944-S7946 (daily ed. Nov. 17, 2010) (statement of Sen. Whitehouse) (“One of the principal findings of our cyber task force was that most cyber threats - literally the vast majority of cyber threats - can be countered readily if Americans simply allowed automatic updates to their computer software, ran up-to-date antivirus programs, and exercised reasonable vigilance when surfing the Web and opening e-mails.”).

See David D. Clark & Susan Landau, Untangling Attribution, 2 Harv. Nat'l Security J. 571, 598 (2011). Former and current government officials, as well as some lawmakers, have stated that the United States should create a new “secure” Internet to eliminate the threats that anonymity poses to the current Internet. Under this proposal, users would need certified credentials to access the new “secure” Internet for critical infrastructure. See Aliya Sternstein, Former CIA Director: Build A New Internet To Improve Cybersecurity, National Journal (July 7, 2011), http://www.nationaljournal.com/nationalsecurity/former-cia-director-build-a-new-internet-to-improve-cybersecurity-20110707.


See Ashcroft Evaluates the War on Terror, CBS News (Feb. 13, 2003), http://www.cbsnews.com/stories/2003/02/13/terror/main340422.shtml; see also Mark D. Young, Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security, 22 Stan. L. & Pol'y Rev. 11, 21 (2011) (“The government is attempting to protect national interests from myriad cyberspace threats and shift its organizational structures to better manage its limited cyberspace resources. It is doing this, however, without adjusting one of the biggest cyber vulnerabilities facing the country: insufficient legal authorities to allow federal action in the cyber domain.”).

United States v. Jacobsen, 466 U.S. 109, 113 (1984) (“A ‘search’ occurs when an expectation of privacy that society is prepared to consider reasonable is infringed.”).

Katz v. United States, 389 U.S. 347, 360-361 (1967) (Harlan, J., concurring) (“My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”); see generally 1 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment §2.1(b)-(d) (4th ed. 2004).


See United States v. Jones, 132 S. Ct. 945, 953 (2012) (holding that placing a GPS tracking device on a vehicle for the purpose of obtaining information is a “search” but that “[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis”) (emphasis in original); see also Illinois v. Andreas, 463 U.S. 765, 771 (1983).

Jacobsen, 466 U.S. at 113.

VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS..., 6 J. Nat'l Security L...
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS..., 6 J. Nat’l Security L....


70 Professor Jack Goldsmith of Harvard Law School finds legal support for a “comprehensive government-mandated, government-coordinated intrusion-prevention system throughout the U.S. network” based, in part, on the “special needs” cases. See Goldsmith, supra note 27, at 6, 11-13.

71 See Hinnen, supra note 3, at 5; see also Goldsmith, supra note 27, at 5 n. 20 (explaining the differences between the “Internet” and the “World Wide Web”).


73 Id. at 623.


75 Id. at 154.

76 E.g., United States v. Ramsey, 431 U.S. 606, 616 (1977) (“That searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration.”); Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) (“It is undoubtedly within the power of the Federal Government to exclude aliens from the country.... It is also without doubt that this power can be effectuated by routine inspections and searches of individuals or conveyances seeking to cross our borders.”) (citations omitted).


78 Id.; see also United States v. Flores-Montano, 541 U.S. 149, 152 (2004) (“The Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.”).


80 Almeida-Sanchez, 413 U.S. at 273 (“A search of the passengers and cargo arriving at a St. Louis airport after a nonstop flight from Mexico City would clearly be the functional equivalent of a border search.”).

81 See 5 LaFave, supra note 49, at §10.5(a) (collecting cases).


83 See United States v. Montoyo de Hernandez, 473 U.S. 531, 538 (1985) (“Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant.”).

84 United States v. Odland, 502 F.2d 148, 151 (7th Cir. 1974) (“There is substantial authority in those Circuits stating the power to search at international borders in the same sweeping terms as the regulation. Any person or thing coming into the United States is subject to search by that fact alone, whether or not there be any suspicion of illegality directed to the particular person or thing to be searched.”).


86 See Dep’t of Homeland Sec., The National Strategy to Secure Cyberspace vii (2003), available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (“Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work.”). See also Clark and Landau, supra note 44, at 574 (explaining that data and electronic communications are transported “on” or “over” the Internet in “packets - small units of data prefixed with delivery instructions” through a “mesh of specialized computers called routers”).
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....

See City of Indianapolis v. Edmond, 531 U.S. 32, 47-48 (2000) ("Our holding also does not affect the validity of border searches or searches at places like airports and government buildings, where the need for such measures to ensure public safety can be particularly acute.").

Ramsey, 431 U.S. at 616.

Cyber attackers often use more than one computer to hide the actual origin of the attack. See Clark and Landau, supra note 44, at 582 ("Many attacks and exploits are multi-stage in character: for example, A penetrates computer B to use as a platform for penetrating C, which is then used to attack D."") (emphasis in original).

See generally R. Marc Kantrowitz et al., Annotation, Validity of Police Roadblocks or Checkpoints for Purpose of Discovery of Alcoholic Intoxication - Post Sitz Cases, 74 A.L.R.5th 319 (2011) (collecting cases).


Id. at 447.

Id.


Sitz, 496 U.S. at 455.

The delay to drivers during the sobriety checkpoints upheld by the Supreme Court in Sitz was twenty-five seconds. Id. at 456. By way of contrast, the delay in the random illegal immigrant checkpoint upheld by the Court in Martinez-Fuerte was three to five minutes. United States v. Martinez-Fuerte, 428 U.S. 543, 543-548 (1976). The federal courts have also concluded that routine traffic stops lasting no more than fifteen minutes are not unreasonable. E.g., Merrett v. Moore, 58 F.3d 1547, 1553 (11th Cir. 1995).


Sitz, 496 U.S. at 451 ("[A]lcohol-related death and mutilation on the Nation's roads are legion."); see also 4 LaFave, supra note 49, at §10.8(d) ("Drunk drivers cause an annual death toll of over 25,000 and in the same time span cause nearly one million personal injuries and more than five billion dollars in property damage.").

Sitz, 496 U.S. at 451 ("No one can seriously dispute the magnitude of the drunken driving problem or the States' interest in eradicating it.").

Id.; see also Delaware v. Prouse, 440 U.S. 648, 658, 663 (1979) (holding that a State's "vital interest" in ensuring "highway safety" could also support "questioning of all oncoming traffic at roadblock-type stops").

Martinez-Fuerte, 428 U.S. at 562 ("Accordingly, we hold that the stops and questioning at issue may be made in the absence of any individualized suspicion at reasonably located checkpoints.").

Cf. Sitz, 496 U.S. at 453 ("The intrusion resulting from the brief stop at the sobriety checkpoint is for constitutional purposes indistinguishable from the checkpoint stops we upheld in Martinez-Fuerte."); see also 5 LaFave, supra note 49, at §10.8(d).

United States v. Martinez-Fuerte, 428 U.S. at 543.

Id. at 554.
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....


106 Id. at 659-661.

107 Id. at 659-660. However, while random stops that involve "standardless and unconstrained discretion" are constitutionally suspect, the Supreme Court did not "cast doubt on the permissibility of roadside truck weigh-stations and inspection checkpoints, at which some vehicles may be subject to further detention for safety and regulatory inspection." Id. at 661, 663 n. 26; see also City of Indianapolis v. Edmond, 531 U.S. 32, 47 (2000) (holding that the constitutionality of checkpoint programs depends on a "balancing of the competing interests at stake and the effectiveness of the program").

108 Edmond, 531 U.S. at 49.

109 Almeida-Sanchez v. United States, 413 U.S. 266 (1973); see also United States v. Ortiz, 422 U.S. 891, 895 (1975) ("Moreover we are not persuaded that the checkpoint limits to any meaningful extent the officer's discretion to select cars for search.").


111 Id.

112 See Michigan Dept. of State Police v. Sitz, 496 U.S. 444, 453 (1990) ("[T]he circumstances surrounding a checkpoint stop and search are far less intrusive than those attending a roving-patrol stop. Roving patrols often operate at night on seldom-traveled roads and their approach may frighten motorists. At traffic checkpoints the motorist can see that other vehicles are being stopped, he can see visible signs of the officers' authority, and he is much less likely to be frightened or annoyed by the intrusion.")(quoting Ortiz, 422 U.S. at 894-895 (1975)).

113 See Martinez-Fuerte, 422 U.S. at 559 ("Motorists using these highways are not taken by surprise as they know, or may obtain knowledge of, the location of the checkpoints and will not be stopped elsewhere. Second, checkpoint operations both appear to and actually involve less discretionary enforcement activity. The regularized manner in which established checkpoints are operated is visible evidence, reassuring to law-abiding motorists, that the stops are duly authorized and believed to serve the public interest.").

114 Delaware v. Prouse, 440 U.S. 648, 663 (1979) ("This holding does not preclude the State of Delaware or other States from developing methods for spot checks that ... do not involve the unconstrained exercise of discretion. Questioning of all oncoming traffic at roadblock-type stops is one possible alternative.").

115 See City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing."); id. at 44 ("We decline to suspend the usual requirement of individualized suspicion where the police seek to employ a check point primarily for the ordinary enterprise of investigating crimes.").

116 E.g., Rice Simmons, The Two Unanswered Questions of Illinois v. Caballes: How to Make the World Safe for Binary Searches, 80 Tul. L. Rev. 411, 413 (2005). According to Professor Simmons, the first reported case to use the term "binary" in connection with a dog sniff was United States v. Colyer, 878 F. 2d 469, 474 (D.C. Cir. 1989) ("As in Place, the driving force behind Jacobsen was the recognition that because of the binary nature of the information disclosed by the sniff, no legitimately private information is revealed: That is, "the governmental conduct could reveal nothing about noncontraband items." ") (citation omitted).


119 Caballes, 543 U.S. at 406.

120 Id.

121 Id. at 407 ("[A] seizure that is lawful at its inception can violate the Fourth Amendment if its manner of execution unreasonably infringes interests protected by the Constitution.").
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS: ..., 6 J. Nat'l Security L...

122 Id. at 410.
123 Id. at 409.
125 Id. at 700.
126 Id. at 698.
127 Id. at 707.
128 Id.
129 Id.; see also City of Indianapolis v. Edmond, 531 U.S. 32, 40 (2000) (noting that a dog sniff is "not designed to disclose any information other than the presence or absence of narcotics").
130 Place, 462 U.S. at 698.
131 Id. at 707.
133 Id. at 29-30.
134 Id.; see also Payton v. New York, 445 U.S. 573, 586-87 (1980) ("It is a 'basic principal of Fourth Amendment law' that searches and seizures inside a home without a warrant are presumptively unreasonable.") (footnote omitted). See generally David E. Steinberg, Restoring the Fourth Amendment: The Original Understanding Revisited, 33 Hastings Const. L.Q. 47 (2005).
135 Justice Souter was concerned with "false positives" that revealed "undisclosed facts about private enclosures, [which would then be] used to justify a further and complete search of the enclosed area." Illinois v. Caballes, 543 U.S. 405, 412-414 (2005) (Souter, J., dissenting). Justice Ginsburg was also concerned that the scope of the initial stop can become unconstitutionally "brosder" if it is not linked to a Terry-analysis. See id. at 419-421 (Ginsburg, J., dissenting).
136 Kyllo, 533 U.S. at 38 ("The [imaging device] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath - a detail that many would consider 'intimate'.")
138 See Simmons, supra note 116, at 438-439.
139 See Kerr, supra note 1, at 1019 (discussing the "content/non-content" line of cases).
140 See Goldsmith, supra note 27, at 11 n. 31 and accompanying text (citing Smith v. Maryland, 442 U.S. 735, 743-44 (1979); Quon v. Arch Wireless Co., Inc., 529 F.3d 892, 904-05 (9th Cir. 2008); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)).
141 See OLC Legal Issues Memorandum, supra note 9, at 3.
142 See infra notes 156-163 and accompanying text for a discussion of a cyber-Terry stop.
143 Cf. O'Connor v. Ortega, 480 U.S. 709, 725 (1987) (plurality) (holding that a search must be "justified at its inception" and "permissible in its scope").
144 United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973). See generally S. LaFave, supra note 49, at §10.6(c).
145 United States v. McCarty, 648 F.3d 820, 824 (9th Cir. 2011) ("[T]he Transportation Security Administration] screens all luggage that goes onto a plane to ensure it does not contain any explosive devices or other items that would threaten the safety of the plane. One
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....

method of screening is through an x-ray device such as the CTX machine used here, which can identify potential safety risks or dense items in luggage that require further inspection.


Davis, 482 F.2d at 913.


United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1246 n. 5 (9th Cir. 1989); cf. Edmond, 531 U.S. at 41 ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.").

$124,570 U.S. Currency, 873 F.2d at 1245.

5 LaFave, supra note 49, at §10.6(e) (collecting cases and noting that passengers are "forewarned by the signs posted in the airport, by the announcement made there over the public address system, or by observation of the search procedures while in the checkpoint line"). While notice to the public and the pervasiveness of government activity can reduce reasonable expectations of privacy, some scholars emphasize that ultimately this question is a "value judgment," and "if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society." Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 403 (1974).

Davis, 482 F.2d at 908 ("Of course, routine airport screening searches will lead to discovery of contraband and apprehension of law violators. This practical consequence does not alter the essentially administrative nature of the screening process, however, or render the searches unconstitutional.").

Some passengers are randomly selected for additional screening "regardless of whether or not the x-ray luggage scan reveals something suspicious." United States v. Marquez, 410 F.3d 612, 614 (9th Cir. 2005).

5 LaFave, supra note 49, at §10.6(e). The "randomness of the selection for the additional screening procedure arguably increases the deterrent effects of airport screening procedures because potential passengers may be influenced by their knowledge that they may be subject to random, more thorough screening procedures." Marquez, 410 F.3d at 614.

Cf. $124,570 U.S. Currency, 873 F.2d at 1245-46 (noting that too "close [of a] working relationship" with "law enforcement authorities" could alter "the calculus" by which airport security searches have been upheld).

See Davis, 482 F.2d at 913 ("In light of that need, a screening of passengers and of the articles that will be accessible to them in flight does not exceed constitutional limitations provided that the screening process is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives, that it is confined in good faith to that purpose, and that potential passengers may avoid the search by electing not to fly.").


Id. at 5-8.

Id.

Id. at 15.

Id. at 20, 27 (holding that a stop and frisk is not unreasonable so long as the officer had a "reasonable belief that he is dealing with an armed and dangerous individual, regardless of whether he has probable cause to arrest the individual for a crime").

Id. at 21, 30. See generally 4 LaFave, supra note 49, at §9.1(b)-(c).

Florida v. Royer, 460 U.S. 491, 500 (1983) ("This much, however, is clear: an investigative detention must be temporary and last no longer than is necessary to effectuate the purpose of the stop. Similarly, the investigative methods employed should be the least..."
intrusive means reasonably available to verify or disperse the officer's suspicion in a short period of time.”); see also United States v. Place, 462 U.S. 696, 709 (1983) (noting the importance of the delay caused by the seizure).


Quarantine and isolation are often used “interchangeably” but refer to different individuals in the physical world. See Kathleen Swendiman & Jennifer K. Elsa, Federal and State Quarantine and Isolation Authority (Cong. Res. Service RL33201), Jan. 23, 2007, at 2. Quarantine refers to individuals who have been exposed to communicable diseases but are “not yet ill,” and isolation refers to individuals that are already “infected.” Id; see also Lawrence O. Gostin, Public Health Law: Power, Duty, Restraint 209-210 (2d ed. 2008) (discussing the differences between quarantine and isolation). This article uses the term quarantine to generically refer to any remedial action that can be taken by the government against a communicable disease in the physical world or a malicious digital code in cyberspace.


Jacobson v. Massachusetts, 197 U.S. 11, 24-25 (1905) (“The authority of the state to enact this statute is to be referred to what is commonly called the police power, a power which the state did not surrender when becoming a member of the Union under the Constitution.”); see also U.S. Const. amend X. (“The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.”).

Jacobson, 197 U.S. at 25; id. (noting that the court has “distinctly recognized the authority of the state to enact quarantine laws and ‘health laws of every description’”) (citation omitted).


42 U.S.C. §9606(a) (2006). Similarly, the Commissioner of the Food and Drug Administration can take measures to prevent the spread of communicable diseases from one state or possession into another in the event that measures taken by state or local authorities are inadequate. See 21 C.F.R. pt. 1240 (2011). The Director of the Centers for Disease Control and Prevention also can take additional measures to “prevent” the “spread of the diseases as he/she deems reasonably necessary.” 42 C.F.R. pt. 70.2 (2005).


Zemel v. Rusk, 381 U.S. 1, 15-16 (1965); see also Compagnie Francaise v. State Bd. of Health, 186 U.S. 380, 397 (1902) (holding that a state law that regulated the introduction of persons and property into a district infested with contagious or infectious diseases was “not repugnant to the Constitution of the United States”); Louisiana v. Mathews, 427 F. Supp. 174, 176 (D. La. 1977) (“Congress has granted broad, flexible powers to federal health authorities who must use their judgment in attempting to protect the public against the spread of communicable disease.”).
See Shapiro v. Thompson, 394 U.S. 618, 629 (1969) ("This Court long ago recognized that the nature of our Federal Union and our constitutional concepts of personal liberty unite to require that all citizens be free to travel throughout the length and breadth of our land uninhibited by statutes, rules, or regulations which unreasonably burden or restrict this movement."). It should be noted that a quarantined individual has the ability to petition a federal court for a writ of habeas corpus pursuant to 28 U.S.C. §2241 (2006).

Compare Smith v. Emery, 42 N.Y.S. 258, 260 (1896) ("The mere possibility that persons might have been exposed to such disease is not sufficient, but they must have been exposed to it, and the conditions actually exist for a communication of the contagion.") (citation omitted), with People ex rel. Barnmore v. Robertson, 134 N.E. 815, 819 (Ill. 1922) ("It is not necessary that one be actually sick ... in order that the health authorities have the right to restrain his liberties by quarantine regulations. Quarantine ... is the method used to confine the disease within the person in whom it is detected, or to prevent a healthy person from contracting the infection."). , and Arkansas v. Snow, 324 S.W.2d 532, 534 (Ark. 1959) (record indicates a "probability that appellee is a very sick person who stubbornly refuses to allow treatment and is probably a source of danger to those around him"); compare Wong Wai v. Williamson, 103 F. 1, 9 (N.D. Cal. 1900) (overturning quarantine regulations during a bubonic plague that were "directed against the Asiatic race exclusively, and by name"), with Greene v. Edwards, 263 S.E.2d 661, 663-664 (W. Va. 1980) (overturning a quarantine law because it failed to accord "procedural due process"), and Ex parte Hardcastle, 208 S.W. 531, 533 (Tex. Crim. App. 1919) ("The law denies to no one restrained of his liberty without a hearing the right to prove in some tribunal that the facts justifying his restraint do not exist."). Some scholars have also suggested additional conditions, including that quarantines must be "reasonable and effective." See Lawrence O. Gostin & Benjamin E. Berkman, Pandemic Influence, Ethics, Law and the Public's Health, 59 Admin. L. Rev. 121, 147 (2007).

See Jacobson v. Massachusetts, 197 U.S. 11, 18 (1905) (holding that the state's implementation of quarantine laws must neither be arbitrary nor capricious); id. at 25 (noting that while the "mode or manner" in which state and local authorities implement quarantine laws is within the discretion of the state, "no rule prescribed by a state, nor any regulation adopted by a local governmental agency acting under the sanction of state legislation, shall contravene the Constitution of the United States, nor infringe any right granted or secured by that instrument").

See Zemel v. Rusk, 381 U.S. 1, 15-16 (1965) (noting that unlimited travel "would directly and materially interfere with the safety and welfare of the ... Nation as a whole").


Sometimes the correct lens is a "hybrid" lens. See Scott J. Glick, FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security, 1 Harv. Nat'l Security J. 87, 110 (2010) ("Foreign intelligence and law enforcement investigations to protect national security [are] 'hybrid' in nature.").

Following a series of coordinated attacks on the London Subway system, New York instituted a security checkpoint program at selected subway stations to systematically search the bags of subway riders for explosives. The Second Circuit upheld the checkpoints under the "special needs" framework; see MacWade v. Kelly, 460 F.3d 260, 268 (2d Cir. 2006). See generally Case Comment, Second Circuit Holds New York City Subway Searches Constitutional Under Special Needs Doctrine, 120 Harv. L. Rev. 635 (2006).

Cf. In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) ("If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government's actions.").
VIRTUAL CHECKPOINTS AND CYBER-TERRY STOPS:..., 6 J. Nat'l Security L....

188 18 U.S.C. §2511(1) (2006) ("Except as otherwise specifically provided in this chapter any person who ... intentionally intercepts ... any wire ... or electronic communication" violates Title III.). FISA also makes it unlawful to intercept communications without an "express statutory authorization." See 50 U.S.C. §1809 (2006); id. §1812 (exclusivity provision).


190 Id. §2511(2)(a)(i) (2006).


192 For example, Congress may conclude that digital scans should only be permitted in regard to malicious digital codes that may be attacking a limited subset of critical infrastructure and key resources, or that the government should be required to make a showing to a court before setting up virtual checkpoints in cyberspace. See also Ric Simmons, Searching for Terrorists: Why Public Safety Isn't a Special Need, 59 Duke L.J. 843, 899-903 (2010) (discussing the role of legislatures in deciding what is "reasonable" under the fourth amendment).

193 See Nojeim, supra note 42, at 119 ("Cybersecurity efforts must be carefully tailored in order to preserve privacy, liberty, innovation, and the open nature of the Internet").

194 Steven G. Bradbury, The Developing Legal Framework for Defensive and Offensive Cyber Operations, 2 Harv. Nat'l Security J. 366, 376 (2011); see John N. Greer, Square Pegs in Round Cyber Holes: The NSA, Lawsfulness, and the Protection of Privacy Rights and Civil Liberties in Cyberspace, 4 J. Nat'l Security L. & Pol'y 139, 141 (2010) ("Many people are rightly concerned when they hear that intelligence agencies will be more active in cyberspace."); Chertoff, supra note 28, at 5 (warning of "dangers" if "the government directly operates civilian domain security, as opposed to simply setting standards for security and enabling private entities to operate the security function in private space").

195 See Greer, supra note 194, at 139.


197 Of course, sending a malicious digital code to attack critical infrastructure and key resources is a criminal offense. See 18 U.S.C. §1030 (2006). As a result, to the extent that forensic examinations and other investigative activities are able to determine the identity of the criminal, under well-established Fourth Amendment principles, the resulting evidence would be the "fruit" of a healthy tree. Compare City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000) ("Our holding also does not impair the ability of police officers to act appropriately upon information that they properly learn during a checkpoint stop justified by a lawful primary purpose, even where such action may result in the arrest of a motorist for an offense unrelated to that purpose."); with Wong Sun v. United States, 371 U.S. 471, 487-488 (1963) ("We need not hold that all evidence is 'fruit of the poisonous tree' simply because it would not have come to light but for the illegal actions of the police."). Professor Simmons, however, argues that suspicionless antiterrorism searches should only be permitted pursuant to the special needs doctrine if the fruits of those searches cannot be used as evidence in a criminal prosecution. See Simmons, supra note 192, at 915-926.

198 Such mechanisms could include "minimization procedures," "ex post auditing and reporting requirements," and a "sunset provision." See Goldsmith, supra note 27, at 15-16.

199 Remedial measures could range from the "least invasive (such as stripping off the malicious code) to most intrusive (destroying the communication)." Id. at 15.


6 JNSLP 97
Reflections on Technology and Intelligence Systems

MICHAEL WARNER*

ABSTRACT The impact of individual technological innovations on intelligence operations is often discussed, but the influence of technological change per se on intelligence systems remains less well understood. The historical literature on this topic is uneven – filled with detailed narratives on certain aspects, but also with surprisingly little attention to larger trends and their meaning. This is significant for two reasons. First, it means we have an incomplete understanding of what happened in the past, particularly for the 'analogue revolution' in intelligence in the twentieth century. Second, it leaves us with few clues for understanding another wave of technological change washing over the intelligence profession at this time (a 'digital revolution'). Looking at the second revolution in the light of the first can give us important clues to what to watch for in coming years.

Technology can be understood as the varying ways in which people consciously and more-or-less collectively create and use tools to manipulate their environment.1 The basic features of technology for any society can be thought of as falling naturally into two rough categories: first, the society’s ‘means of production’ (the mechanisms and methods by which its members shape their physical surroundings and accumulate wealth); and second, its artificial means for recording and communicating information (i.e. its collective understanding of how to collect and use data in making decisions). The relative abilities of neighboring societies to employ both aspects of technology will be of obvious interest to any society desiring to divine their neighbors’ plans.

Despite this relevance, technology’s impact on intelligence has been incompletely examined. To be sure, there is no lack of interest in the topic. A quick Google search yields more than 9 million hits for the phrase ‘technology and intelligence’. Although most of these references seem to relate to topics in the field of technology and human cognition – and not to intelligence in international affairs – still the reading list for intelligence professionals and observers must be vast.

*Email: warner@american.edu

1Wikipedia’s article on Technology tells us it is ‘the making, usage, and knowledge of tools, machines, techniques, crafts, systems or methods of organization in order to solve a problem or perform a specific function’ (accessed 8 December 2011).

ISSN 0268-4527 Print/ISSN 1743-9019 Online/12/010133-21 © 2012 Taylor & Francis
http://dx.doi.org/10.1080/02684527.2012.621694
If such a list could ever be compiled, however, the preponderance of the
titles on it would surely pertain to 'intelligence technology'. Hundreds of
authors have discussed individual innovations used by intelligence officers
and agencies; indeed, one need only recall the many popular books and
articles on 'spy gadgets' to grasp this point. This literature has had a long life
already. A collective fascination with the tricks of espionage seems to have
been well noticed by the publishing trade as early as the 1930s. That
trend shows no signs of abating, as the popularity of the for-profit 'International
Spy Museum' in Washington, DC, might attest.

A small but significant subset of the literature on gadgetry has sought by
scholarly methods to explain the genesis and impact on intelligence
operations of various innovations. The mathematical and computational
wizardry employed by the Allies to break German and Japanese codes in
World War II has attracted considerable interest from scholars. Reconnaiss-
sance by intelligence services and the aircraft and other systems they have
used to conduct it has garnered steady attention as well. Both of these broad
topics emerged as scholarly emphases after memoirs by participants helped
prompt and guide the declassification of official histories and documentation
that began in earnest during the 1970s. That release of selected facts and
records took place chiefly as a result of actions taken by the American and
British agencies that developed and utilized the tools in question during the
world wars and the early Cold War. Although the new knowledge of how
progress in signals and imagery intelligence affected the organizations that
developed and used these techniques pertained largely in an Anglo-American
historical context, some of the lessons to be drawn seemed applicable more
broadly, if not universally.

An even smaller branch of the literature treats technology as an
intelligence target. The best of these titles on 'technology intelligence' cover
the use of secret sources and methods to understand the scientific and
technological plans and capabilities of adversaries. R.V. Jones (1911–97)
helped to pioneer this field, both as a scientific adviser to the British high
command in World War II and later as a memoirist; his published reflections
provide an excellent introduction to the principles and patterns of this sort of
work. Narratives like his read almost like detective stories, in that they
involved puzzles and clues and end in satisfying (or at least logical) solutions.

These different sorts of writings discuss technology as a tool — or a target —
of intelligence. Some of them mention specific ways in which intelligence
officers and agencies have had to shift talent or resources to new problems
posed by an enemy's technological innovation. Others discuss how new

---

2See, for instance, the breathless descriptions of real and fancied spy gear in Richard Wilmer
Rowan, Spies and the Next War (Garden City, NJ: Garden City 1956).
3Two such memoirs were Frederick W. Winterbotham, The Ultra Secret (New York: Harper
& Row 1974); and Constance Babington-Smith, Air Spy: The Story of Photo Intelligence in
4R.V. Jones, The Wizard War: British Scientific Intelligence, 1939–1945 (New York:
Coward, McCann, & Geoghegan 1978).
Reflections on Technology and Intelligence Systems

offices and sometimes whole agencies came into being to develop, deploy, and exploit some breakthrough invention promising military or intelligence advantages over adversaries. The value of such studies cannot be disputed; they have opened new windows in the hitherto secret world of espionage. Nonetheless, that value has limits. Few works on technology and intelligence examine or add to our understanding of how technology affects intelligence ‘systems’ – the collective authorities, resources, personnel, and tasks that a nation allocates to using secret means against real and potential opponents. Here is a gap in the scholarship, and an opportunity.

Technology and Intelligence

A state’s technological environment will have both direct and indirect causal relationships with the ways in which a state tasks and organizes its intelligence offices. This relationship shows most acutely in military matters. Because so much intelligence work is devoted to managing competition or winning active and potential conflicts with other states, the way in which a state applies violence in an organized manner to achieve its objectives will shape, in important ways, its intelligence system. The organization, mobility, and lethality of a state’s military – and those of its adversaries – will dictate (among other factors) the timeliness and precision demanded of intelligence work, the expertise that must be devoted to understanding what intelligence collects, and possibly the relative importance of human versus technical means of collection and dissemination. Technological change shapes and re-shapes both the threats to a state as well as the opportunities available to it in the international arena, and thus it plays a role in determining the targets of intelligence and the means that intelligence employs. It also helps to determine the numbers and sorts of intelligence officers hired to collect and analyze data as well as to disseminate the resulting reports to decision-makers. Finally, it has direct impacts on the structure of intelligence organizations and their institutional relationships.

Technology’s effects – and thus its influence as an independent variable in shaping a state’s intelligence system – can be seen best over time. Such effects upon intelligence systems manifest themselves most dramatically in the midst of rapid and profound technological change, and yet there is no William H. McNeill to explain how technology affects intelligence as such. McNeill’s 1982 classic The Pursuit of Power examined the sustained impacts of technological change on the military arts and the ways in which they expanded or altered the relative capacities of commanders and societies to impose their will on others. He was not the first or the last author to take such an approach; one thinks of Elting Morison before him, and other authors like Jared Diamond in recent years. Still, McNeill may be without superiors in his reflections on the complicated interplay between organizations, finance, innovation, and war-making, showing how technological

---

change made possible advances in armaments and tactics, which in turn forced revisions to national strategies – sometimes by opening significant opportunities for gains at the expense of rivals.

McNeill's insight has its merit in showing how the advantages of technical innovation have tended to accrue to militaries and societies that are open to change and organized to take advantage of it. Those societies notice the value in a new device or technique – like cannons or close-order drill – because they already have pre-existing habits, institutions, or inclinations that can be adjusted to adapt and spread it. They are also the ones to take advantage of the new cycles of innovation and adaptation that some inventions initiate. When their openness to innovation reaches its limits – whether for cultural, religious, or material reasons – a society's technological prowess can plateau, or even decline.

Several authors have provided hints of the insights that can follow from taking a similarly 'systemic' approach to studying the effects of technological change on intelligence. David Kahn's seminal study *The Codebreakers* (1967) showed how the intelligence profession in the West followed innovations in communications technology, becoming mechanized and industrialized as nations shifted from couriers to telegraph to radio (and from amateurish codes to machine encipherment to protect their messages). Kahn devotes ample space to the geniuses and skullduggery that inevitably enliven this story, but the real point of *The Codebreakers* is that method usually trumps intuition; plodding and careful routine – endlessly repeated across an entire agency, service, or government – provides nations sufficient security for their communications and (occasionally) the ability to read the messages of their rivals. The organizations that can establish and replicate these methods are those that render the best service to the decision-makers who rely on them – and thus are more apt to be given the resources and authorities they can use to grow in size and influence.

Recent works by scholars such as Jonathan Winkler and David Nickles have added new depths of insight. Winkler and Nickles chose different vantage points to chart the emergence of global telecommunications and show its effects on both diplomacy and military command and control, and, most important, on national strategy. The opportunity to communicate more swiftly and more securely in the nineteenth century transformed itself almost overnight from a luxury for diplomats to a necessity for entire governments. That development in turn dictated a host of strategic consequences, from state investment in cable companies and raw materials to competition over the rights to beaches where undersea cables could 'land'. Both Winkler's and Nickles' contributions illuminate the complex and inter-related ways in which technological innovation

---

affected diplomacy, operations, and strategy — and also intelligence gathering, organization, and planning more generally.

John Ferris has explored the impact of communications technology on intelligence more directly. Treating topics as varied as British air defense against Zeppelin raids and the concept and effects of ‘C4ISR’ in Operation Iraqi Freedom, he has demonstrated how new weapons, intelligence practices, and command and control systems can interact in ways their designers never expected. Once set in train by the exigencies of military campaigning and the need to counter enemy initiatives, these interactive processes transformed intelligence practices and intelligence agencies — particularly by making them demand, consume, and produce vastly more information faster than ever before. Information becomes — in Ferris’ larger narrative — the animating force behind military innovation and operations: to control its use (and deny it to enemies) became the object of a large share of the energies of modern business, government, and military systems. The intelligence systems of the states controlling such capabilities have been pulled along in the wake of this sweeping re-ordering of military (and hence national) priorities, growing and being transformed to support actual and potential combat operations.

The United States’ then-Director of National Intelligence, J. Michael McConnell, attempted in 2008 to address related issues from a different vantage point in a public document titled Vision 2015. His essay marked an unsystematic but thoughtful portrayal of the future that awaits the US Intelligence Community. Vision 2015 attempted to foresee not the political and economic events that will affect various nations, movements, and regions, but rather the global trends that are changing the ways in which the Intelligence Community will collect, analyze, and share information. Those trends, said Vision 2015, will both challenge current practices and provide opportunities for new and better ones. The speed and volume of data flows — and the need to understand them faster than determined enemies or adverse trends can harm Americans or damage national interests — places an imperative on changing the ways in which the Intelligence Community organizes its people and efforts. In short, the US intelligence agencies that had been created, organized, and tasked

---


*C4ISR* signifies ‘command, control, communications, computers, intelligence, surveillance, and reconnaissance’.


along the lines of the various collection ‘disciplines’ (human intelligence, signals intelligence, and the like) and functions (collection, analysis, and dissemination) should find ways of training, equipping, and managing the bulk of their officers in networked (and ever-shifting) inter-agency and inter-disciplinary task forces dedicated to addressing particular intelligence targets.

Intelligence is too marginal and secretive to have sweeping effects on society writ large like those described by McNeill – the influence flows mostly the other way. Nonetheless, these explorations of McNeill, Kahn et al. collectively suggest that the evolution of technology should be a prime subject of intelligence studies. It is time to look more carefully at technology and intelligence systems. In theory, the technological ‘environment’ can affect the ways in which a state tasks and organizes intelligence systems in varying ways. Changes in technology, by altering both threats to the regime and opportunities available to it, help to determine the objects of intelligence, the means that intelligence employs, and the ways in which it organizes those means. The technological context of an intelligence system can be assessed with reference to several factors that are of particular relevance to what follows:

- the society’s means for producing and distributing goods and services; in short, the level and sophistication of its overall economy;
- the level and reach of a society’s methods for creating, sharing, and retaining information; and,
- the ways in which a society can employ to maintain order within its boundaries and impose its collective will on other societies; to wit, its military means and prowess.

These factors all affect the structure, tasks, instruments, and targets of an intelligence system in several ways, as can be seen in what are perhaps the two most important historical examples of discontinuous shifts in intelligence systems wrought by technological change.

Learning By Example

World War I precipitated what might be called the ‘analog revolution’ in intelligence. Before the invention of radio and aerial photography, intelligence could still be conducted in ways essentially unchanged since the beginning of history. Sun Tzu (ca. 300 BC) discussed how commanders could gain information on their enemies and use intelligence means to blind and mislead them. To cite another example, Kautilya (ca. 200 BC) explained how very similar methods could be used to guard the regime and allow a prince to confuse and defeat his domestic as well as his foreign

---

enemies. A very long period of military innovation and social change did not essentially alter this instrumental and very limited concept of intelligence. It is true that industrialization, mass armies, and steel ships created a hunger among nineteenth-century armies and navies for information on their real and potential enemies (and the locales where they might have to fight them). This need brought forth the initial, small military and naval intelligence bureaus that most Continental powers and the United States had created by 1900. The technological means for gathering such intelligence—and hence the sophistication of the staffs involved in it—was not per se different from what could have been done in Napoleonic (or Roman) times. One can glimpse this point by perusing an 1895 treatise published by a British staff officer, Col. George A. Furse. His discussion of intelligence added the telegraph, newspapers, and filing cabinets to the means available to the commander-in-chief and his intelligence officer—but did not differ in its essentials much from Sun Tzu.

Beginning in 1914, intelligence in the major European powers swiftly evolved from being a secret annex to the state's security, diplomatic, and reconnaissance functions, and matured into its own quasi-profession, populated with specialists laboring in bureaus custom-organized for their work. Radio and aircraft observation were the chief spurs to this revolution as the fighting spread from the land and sea 'domains' to the air as well. War had become a vast consumer of materiel during the Industrial Revolution, and now seemingly overnight it became a geometrically greater consumer of information as well, with the possibility of real-time transmission of orders, reports, and data almost immediately becoming the imperative to do so faster and more accurately than one's adversary—who was also racing to overtake his own adversaries. The sudden and urgent need to exploit radio signals and photographic images to learn the enemy's disposition and divine his intent created wholly new intelligence disciplines. Men (and very soon women as well) with little or no prior training in these crafts became specialists, and the services that gathered them together to parse intercepted transmissions and scrutinize aerial photographs applied the maturing principles of organization to create, as it were out of whole cloth, entire new intelligence bureaucracies where nothing of the sort had ever existed before.

Each of the major powers in the conflict had to follow suit for their own protection. The new disciplines of signals intelligence and imagery intelligence led the way on the Western Front in France (and in an England at risk from German bombing raids on its cities). Their corps of analysts and technicians had to be organized in increasingly complex, industrial-age offices and staffs, complete with intricate divisions of labor, precise support and logistical services, hierarchical management structures (and sometimes

\[12\] I discuss both of these ancient authors in 'The "Divine Skein": Sun Tzu on Intelligence', *Intelligence and National Security* 21/4 (2006).

with around-the-clock production cycles) to process data and disseminate their products to their patrons and ‘customers’. Furthermore, someone had to manage these workers and offices – hence American pioneer cryptologist Herbert Yardley’s lament that ‘it began to look as if the war had converted me into an executive instead of a cryptographer’. 14

The First World War set in motion changes that would carry themselves toward their logical conclusions in the other great conflicts of the twentieth century. By World War II, industrial-scale signals intelligence and imagery intelligence for commanders were supplemented by theater- and national-level signals intelligence (sigint) and imagery bureaus to produce intelligence for decision-makers far from any battlefield. 15 As the central problem of intelligence turned from gleaning scarce clues to coping with the glut of data, this ‘analog revolution’ empowered the richer states that could afford the mass-production intelligence systems that it made possible, giving them distinct (if sometimes fleeting) diplomatic and military advantages over more backward allies and competitors.

The intelligence innovations of the Cold War, for the most part, deepened and broadened the changes that had been set in motion in 1914. The only real intelligence collection discipline to be added – ‘scientific intelligence’, or as it is sometimes called, ‘measures and signatures intelligence’ (MASINT) – was a refinement on the collection of data emitted in the electro-magnetic spectrum; thus it was closely related to signals intelligence and imagery intelligence. In addition, the sophisticated collection ‘platforms’ of the Cold War – U-2s, SR-71s, spy satellites – were just that: platforms. They carried cameras and instruments that had descended directly from their relatively crude ancestors deployed with the armies that fought in the First World War.

In sum, one can tally six major effects resulting from the analog revolution that began in World War I:

- A revolution, by definition, means there is no going back to old ways. After 1914, any nation desiring to project power beyond its borders had to build new, larger intelligence organizations based on industrial methods of resourcing, processing and distributing product. As a corollary, a revolution also entails the dynamic of ‘creative destruction’, in which rapid technological and organizational changes place a premium on agility, adaptability, and innovation. Those who cling to old ways, or fail to take appropriate countermeasures, are defeated or pushed aside as their decreasing effectiveness becomes ever more glaring (and dangerous). The aforementioned Herbert Yardley, ironically, fell victim to this himself in the 1920s, as new methods of machine

encipherment outstripped his essentially pencil-and-paper codebreaking operation.16

- Making sense of large quantities of data as fast as possible suddenly became imperative, forcing the birth of something new: data management, with analysis and analysts. This soon began to revolutionize both military operations and military intelligence.17 Since for the most part the new organizations created to process signals or imagery were situated in military structures, this need for analysis and analysts caused something of a cultural shock to those same militaries, which were forced to hire and also to protect and promote all sorts of distinctly un-military persons.18 Official reflections on this topic during World War I sound amusing in hindsight. The head of the American Expeditionary Force’s sigint section (G-2/A-6), Frank Moorman, noted in 1917 that the Army suddenly needed men of the sort who had 'spent their lives studying hieroglyphics, cuneiform characters and the like'.19 One can imagine how such advice must have struck some of his superiors and colleagues, trained as they were for an era of black powder and cavalry charges. In addition, the Commonwealth allies and the United States intelligence systems by the end of World War II had mobilized their universities to create a new institutional discipline – ‘all-source analysis’. These new analysts pieced together fragments of information to fashion mosaic pictures of the intentions and capabilities of opponents.

- Asymmetric progress between security measures and collection systems meant huge vulnerabilities suddenly opening and closing. That unevenness was the cause of both joy and grief. Particularly in wartime, victory could swing toward the first antagonist who identified and exploited (or closed) the breaches created by well-intentioned but flawed innovations in communications and operational security. Both sides drew lasting impressions from the battle of Tannenberg in 1914, at which German generals read Russian orders radioed en clair and used them to thrash

---


19Frank Moorman, Office of the Chief of Staff, American Expeditionary Force, ‘Notes on Personnel Required by Radio Intelligence Service, AEF’, no date (1917), National Archives and Records Administration, Record Group 120, American Expeditionary Force, Entry 105, Box 5765, unnamed folder. I am indebted to Mark Stout of the International Spy Museum for this reference and citation, as well as other insights he kindly shared with me in drafting this article.
two Russian armies before they could join forces. 'We were always warned by the wireless messages of the Russian staff of the positions where troops were being concentrated for any new undertaking', bragged German general Max Hoffmann in his 1924 memoir. 'Only once during the entire war were we taken by surprise on the Eastern Front by a Russian attack'. The signals intelligence triumphs now known by the shorthands of ULTRA, MAGIC, and Venona are only three of many notable examples that need no elaboration here.

- Intelligence sharing with industry and coalition partners became crucial to the performance of intelligence services for perhaps the first time in history. This phenomenon had both positive and negative aspects. Collection, processing, evaluation, and analysis all benefited from the economies of scale and divisions of labor made possible if intelligence bureaus could acquire custom-built equipment and collaborate across national lines. In addition, allies had to have roughly parallel intelligence capabilities for their mutual protection. For instance, the British and French felt compelled to teach the new intelligence skills to their new allies as quickly as possible in 1917 as the American Expeditionary Force prepared to take over sectors of the Western Front. A senior American intelligence officer shortly after the war remembered that the British were very anxious that they would make us understand how serious all these things were. The French had the same solicitude but they were less tactful in expressing it ... Their attitude was more 'Well, this is the way it is, you can take it or leave it.' The British attitude was 'this is the way it is; for God's sake take it, take our word for it'.

The three-way sharing of intelligence that resulted — while crude by later standards — nonetheless benefited all partners, and created precedents for the great Anglo-American intelligence alliance of World War II and beyond.

- The management of the relationships between the new intelligence collection and production offices also became very important. Large,

---

20 Quoted by Kahn in The Codebreakers, p.633. American cryptologist William Friedman was still citing Tannenberg as an object lesson for National Security Agency employees more than four decades later; see the collection of his lectures published as The Friedman Legacy: A Tribute to William and Elizabeth Friedman (Pt. Meade, MD: National Security Agency 2006) p.123.


specialized organizations the world over tend to go rent-seeking; i.e. to channel resources to activities that bring in new resources at a minimum of risk and disruption, and the new intelligence bureaus were no exception. Methods and mechanisms for the internal oversight of secret activities thus needed to be created, with ‘metrics’ for assessing performance as well. Who best to manage such enterprises was another serious question: should the leadership ranks be staffed with the geniuses who made the breakthroughs in the first place, or with trained executives who could make the accounts balance (but who might be less sensitive to the operational or technological details)?

- Finally, nations that build technologically sophisticated, multi-agency intelligence systems sooner or later find that intelligence can never seem to meet all the needs placed on it by national, operational, and tactical decision-makers. The expense and difficulty of constant monitoring and collection, and the associated processing, analytical, and dissemination costs, made the new signals and imagery collection ‘architectures’ unique; they could not be replicated for multiple users. In other words, a single intelligence architecture had to serve both national and departmental customers. That meant there had to be an exquisite balancing of efforts, resources, and targets. How then to satisfy the competing needs of both national and sub-national officials and commanders for intelligence support capabilities that were too sensitive and expensive to duplicate for both sets of requirements? In the Cold War this problem of management became even more acute, especially for the United States with the development of satellite-based collection platforms. In addition, as technological sophistication in the intelligence field increased, the spiraling costs involved with deploying advanced collection systems grew to be another significant factor driving the administration of intelligence systems. The many issues involved in managing complex collection and analytic systems to support warfighters, ministers, and policymakers will continue to be felt for as long as collection technologies remain so costly and rare.

The Digital Revolution

The rapid development of the military art in the early twentieth century has significant parallels – and some instructive points of dissimilarity – with the revolution in information technology and intelligence now sweeping the globe. The rapid progress of science in modern times owed much to the realization that mathematics could play so much larger a role in helping mankind understand the natural world than had hitherto been suspected. Similarly, the information revolution took off in the 1940s with the realization that any task could be subjected to mathematical processes (with their accompanying speed, volume, and precision) if it could be

---

23I discuss an instance in which this dilemma had practical effects in ‘Reading the Riot Act: The 1971 Schlesinger Report’, Intelligence and National Security 24/3 (2009).
expressed in the form of an algorithm. The result has been an accelerating shift of work and communications tasks to computerized (i.e. digital) processes, swiftly followed by an equally momentous connecting of these processes to one another over networked channels. If the analog revolution was a discontinuous shift in the technology of acquiring and sharing information, then its digital counterpart represents yet another: discontinuous shift in the technology of acquiring, sharing, and storing information. Its effects are still emerging and their outcome is difficult to predict, though their significance for intelligence systems can be expected to be profound.

The digital revolution's impetus is the tectonic confluence of three developments in what we have collectively dubbed 'cyberspace': the interlinking of mankind via cheap and seemingly instant, relatively secure, and ubiquitous communications, the shift of humanity's collective memory and data processing into increasingly capacious and accessible electronic archives, and the 'democratization' of innovations that can cause narrowly tailored or widespread economic or even physical harm (i.e. viruses, worms, and other forms of 'malware'). Every government and intelligence system is feeling the effects of this digital revolution. Concepts, organizations, and doctrines that intelligence systems had created and maintained during the analog revolution of the twentieth century now have to be revised. Moreover, they have to be revised rapidly while the systems around them are still performing their intended missions. As one senior Bush administration official in Washington noted while the US Intelligence Community was being reformed in 2004, doing so is like undergoing surgery while galloping on a horse.\(^{24}\)

To understand these changes and their effects, it might be useful to compare the impact of the current information revolution with that of the last one. Almost as soon as people began transmitting information via wireless, their adversaries began eavesdropping on and/or disrupting the transmissions, thereby forcing all sides to undertake to secure their own use of radio from foreign prying or tampering. These three activities—'exploit, attack, and defend'—apply to the world of digital data transfers just as they apply to the realm of radio, with an added twist: radio signals exist only when they are transmitted, while data storage at both the sending and receiving ends means that data can be attacked or exploited (and therefore must be defended) when they are at rest as well as when they are in transit. These parallels between radio and cyberspace suggest that the points made above concerning the analog revolution have parallels today:

• The digital revolution, like the analog, is at its root an irreversible transformation of how people acquire and use information. That fact has immediate ramifications for intelligence – much of which, after all, concerns the discovering of that which others know (or think they know). How those others acquire, store, transmit, and secure such information, therefore, is of fundamental importance to intelligence in all eras – indeed, it will dictate at a basic level the tactics and techniques of intelligence, which – in that sense – can be thought of as a function of the changes in information technology. Today the ‘things’ that people, enterprises, governments, and societies value are increasingly not things at all – but rather are units and arrangements of information – ones and zeroes – more and more often created, stored, moved, and shared by digital means. One particular aspect of this topic merits additional consideration. Intelligence naturally follows wealth: where value and hence wealth are created, stored, moved, and shared, there is where intelligence services will employ secret means to divert some of that value for their own purposes (and where the rightful owners will deploy overt and covert means of their own to stop such diversions).

This is already happening on an impressive scale, if one credits press reports on the ‘GhostNet’ discovered by University of Toronto researchers; this operation, which the investigators deemed to be of Chinese origin, over a span of two years penetrated at least 1295 computers in 103 countries, ‘including many belonging to embassies, foreign ministries and other government offices’.26

• The digital revolution creates everywhere a much greater demand for analysis, and analysts. The volumes of data that can be moved, stored, or stolen, are simply astronomical – they can barely be comprehended, let alone utilized by current methods. In short, the collection of digital information by digital means can easily outstrip the ability of analysts to sort through the take. For instance, Maj. Gen. William Lord, then of the US Air Force’s Office of Warfighting Integration, claimed at a public conference in August 2006 that Chinese hackers had downloaded ten to 20 terabytes (TB) of data from the Department of Defense’s Non-Classified IP Router Network (NIPRNet).27 Such a statistic is both

---


awe-inspiring and puzzling. Who can possibly digest 10–20 TB, which at a good reading speed of 200 words per minute (or 2.5 kb of file space in text files) might take 3333 to 6666 work years (each of 50 work-weeks of 40 hours each) just to read? The answer is that analytical processes themselves are being swept along in the digital tide. They began to be automated (or at least assisted by desktop computing) in the 1980s, and now are being compelled to become much faster and more capable to keep up with the volume produced by automation elsewhere. There is already a vast literature on the technical and social factors involved in linking databases within and across organizations and the sorting and searching of their contents – the imperative to accomplish these feats with ever-greater speed and accuracy is now demanding a high share of mankind’s creative energies. The fact that intelligence professionals and their agencies are decidedly not among the leaders of this movement suggests that commercial firms like Google may well foster and train the next generation of path-breaking intelligence analysts – many of whom might not place their skills at the service of their respective governments.

- Organizational reshuffling is being forced by technological shifts as the preponderance of resources, taskings, and authorizations shift from older intelligence targets and methods to newer ones. The digital revolution radically compresses the time intervals available for recognition, decision, discrimination, and action – sometimes to milliseconds. A race is on to figure out intelligence organizations and doctrines for the digital age. That management challenge transcends all intelligence systems and indeed touches every large knowledge-based enterprise in the post-industrial age. No nation or enterprise has fully solved the problems of productivity and accountability associated with the new digital means, so it is doubtful that intelligence agencies, which typically take on their organizational models from their social contexts (rather than vice versa) will innovate for the whole of post-industrial society in this case.

- As with the analog revolution, success favors coalitions. Though there is little information publicly available on transnational intelligence partnerships in cyberspace, one could probably argue cogently from the precedent of the analog revolution that any strictly ‘national’ intelligence system (one with no significant liaison partners) is by nature at a serious

---

28 Some idea of the magnitude of this literature can be gained from a quick perusal of Wikipedia’s listings under the Category ‘Databases’, which holds 13 sub-categories and 186 separate ‘pages’ (i.e. individual articles). Choosing only a single one of those sub-categories, ‘Knowledge discovery in databases’, one finds under it a further two sub-categories and 15 pages.

29 Another question also arises: could the tools those analysts employ subtly constrain their thinking and thus their analyses? This is no trivial matter in an intellectual milieu in which ideas are typically expressed in formats dictated by (or compatible with) Microsoft Office software. I thank Martin Alexander for raising this issue, which might one day demand considerably more attention and insight than the present author can bring to it.
disadvantage against sets of intelligence systems that collaborate against common targets.

- Another parallel can be seen in the rapid spread of general knowledge about the new changes. We noted above Max Hoffmann’s boast about German exploitation of Russian wireless. His memoir was one of several accounts published in the 1920s that publicly revealed the importance of signals intelligence in World War I.\(^{30}\) The digital revolution in intelligence has had a similar run of early publicity. Der Spiegel noted in 1969 what might have been the first example of computer espionage (perpetrated by the ubiquitous Markus Wolf); Clifford Stoll’s The Cuckoo’s Egg (1989) remains a classic and timely account of a remote access operation; and James Adams explained in 2001 how foreign hackers had seemingly taken up residence in sensitive US government networks.\(^{31}\) What seems new can be much older than commonly thought.

- Finally, and despite the general knowledge of what is happening, progress in particular areas can be quite asymmetric. Just because something is ‘public’ does not mean everyone has noticed it or realized its implications. This probably does not need elaboration; as science-fiction writer William Gibson likes to say, ‘the future is already here. It’s just not very evenly distributed’.\(^{32}\) As in the two world wars, the intelligence system that spots its own vulnerabilities and those of adversaries (assuming it patches the former and exploits the latter) is going to have clear advantages. Success in this realm probably favors the side that is more self-critical and more open to external oversight.

**Two Disparities**

To grasp the implications of new information technology (and the whole panoply of social and economic changes it has wrought) on intelligence structures, one might also consider two developments that do not seem to be well explained by the above parallels between the analog and digital revolutions:

---


First, the new course of technology seems to be erasing the already blurry state/non-state actor line, putting powerful and stealthy weapons in private or non-state hands. Digital technology has given virtually all nations— and even angry and determined groups and individuals— suites of intelligence capabilities that since the dawn of the analog revolution had been virtually monopolized by the richer and more advanced states (and their clients). Today the digital revolution makes some forms of intelligence and security more expensive; witness the fanfare that greeted the announcement in October 2009 that the US National Security Agency (NSA) would build another large data center—this one a $1.5 billion effort in the state of Utah. At the same time, however, it makes other forms of intelligence much cheaper; small states and non-state actors can now practice espionage and covert-action against the largest states, with comparatively little expense and minimal risk to themselves. Attacks can be very difficult to attribute to specific attackers, who can mobilize vast numbers of computers owned by unwitting bystanders into ‘botnets’ that support specific activities. This lowering of what economists call the barriers-to-entry for intelligence trends in the opposite direction from the changes set in motion during World War I, which had concentrated information power and destructive weaponry in state hands. Here is another effect of the digital revolution that may merit two considerations from future students of comparative intelligence systems. First, are we approaching a time when it is possible to duplicate ‘national-level’ collection capabilities for each department or agency that wants them? Perhaps not, but that does not mean that some ministries or departments


34 James Gosler explains the problem of attribution thus: ‘For low-level threats, such as hackers, the combination of a connected target and an inherent vulnerability is sufficient to exploit targets... In the recent past, US adversaries have collected and exfiltrated several terabytes of data from key Department of Defense networks. The apparent inability to patch US systems in a timely manner provides opponents with ample opportunities for access to our information systems. While we are aware of these operations, we do not appear to have the technical ability to close the access holes or to clearly attribute these operations to the perpetrator(s)’ [punctuation in original]. See Gosler’s ‘Counterintelligence: Too Narrowly Practiced’ in Jennifer E. Sims and Burton Gerber (eds.) Vaults, Mirrors, and Masks: Rediscovering US Counterintelligence (Washington, DC: Georgetown University Press 2008) pp.181–2.

might not attempt to create their intelligence capabilities for their own specialized needs in cyberspace. Second, will we see more ‘super-empowered’ individuals like Henry Okah, the Nigerian warlord who from South Africa and other nations used his cellphone and the internet to build, arm, command, and advertise the Movement for the Emancipation of the Niger Delta (MEND)?

It is not difficult to imagine such entrepreneurs of violence building their own sophisticated intelligence operations to support their plans; one might argue that Al Qaeda already has.

• Second, leaders and communicators during the analog revolution did not have to worry as much as they do now about the integrity of the data being transmitted. The fact that our computers now transmit and store data means that those data can be stolen or corrupted whether in motion or at rest. Then-US National Counterintelligence Executive Joel Brenner indirectly reflected on this in a 2009 speech, noting that

We’re also seeing counterfeit routers and chips, and some of those chips have made their way into US military fighter aircraft ... you don’t sneak counterfeit chips into another nation’s aircraft to steal data. When it’s done intentionally, it’s done to degrade systems, or to have the ability to do so at a time of one’s choosing. There is no longer a meaningful difference between data security and operational security. Our operations depend on our networks – the same networks on which we create, move, and store data.

The imperative to protect the integrity of data and ensure the computers they reside on can be trusted to guard them has given rise to the field of ‘information assurance’, which Bruce Schneier described as confidence that ‘a system does what it is supposed to do, and doesn’t do anything else’. Glenn Gaffney, former Deputy Director of National Intelligence for Collection in the US Intelligence Community, explained the central problem for information assurance as follows:

---


In fact, you don’t have to corrupt any information to corrupt all of it. The nasty side of the integrity breach is that all the code/data contained within the system is rendered suspect. Just the fact that an adversary has been present in your system makes the entire system suspect. The depth of the risks associated with the integrity issue and the potential costs for recovery are frightening.39

Levels and Domains

A decade ago strategists and military historians debated whether digital technology and networking had fostered a ‘Revolution in Military Affairs’. Networks would soon fight networks in non-kinetic conflicts, it appeared; and where live forces engaged, intelligence, command, and action would be fused by all-but omniscient sensors and instant and ubiquitous control. The wars in Iraq and Afghanistan, however, seemed to have settled the issue in the pessimists’ favor. War had not changed – it was still the same gritty business it had always been, albeit with more accurate weaponry and timelier communications.40

This verdict would seem just if ‘cyberspace’ is considered as merely a domain of military operations, resembling the land, sea, and air domains as spaces through which forces assemble, communicate, and move, and in which they engage one another. That is indeed how the Joint Chiefs of Staff now views it, as evidenced in their 2004 National Military Strategy, which asserts ‘The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace’:41 Indeed, the US military’s new Cyber Command – with its commander serving simultaneously as the Director of the National Security Agency – will be the entity charged with ensuring such freedom of action for the United States in the cyber domain.42

42 According to Ellen Nakashima in the Washington Post, the new US Cyber Command would ‘merge the Pentagon’s defensive unit, Joint Task Force-Global Network Operations, with its offensive outfit, the Joint Functional Command Component-Network Warfare, at Fort Meade, home to the NSA. The new command, which would include about 500 staffers, would leverage the NSA’s technical capabilities but fall under the Pentagon’s Strategic Command’; see ‘Pentagon Computer-network Defense Command Delayed by Congressional Concerns’, Washington Post, 3 January 2010, p.A04. See also Lieutenant General Keith B. Alexander’s answers submitted before his 15 April 2010 Senate confirmation hearing to be the first commander of Cyber Command, <http://www.fas.org/irp/congress/2010_hr/041510alexander-qfr.pdf> (accessed 24 April 2010). Israel’s chief of military intelligence,
But cyberspace is not a place at all, and thus cannot be considered simply as a domain for military activities (useful as that insight can be). Every bit or byte exists because someone directly or indirectly created it. Cyberspace is the product of human action, a realm for human action, and the current expression of those actions. Unlike the traditional military domains, it has its being outside of time – there is no past or future in cyberspace, there exists only the activities that people have individually and collectively caused to be happening at this instant. Those activities and the events they cause can manifest themselves as hostile acts, in that they cheapen and sometimes destroy the value of information and networks. Such acts need to be regarded as points on the continuum of conflict that ranges from diplomacy through coercion, terrorism, asymmetric warfare, and conventional warfare, to the ultimate use of weapons of mass destruction. They would seem to lie mostly on the less-destructive end of the conflict continuum, but that should give no comfort to statesmen and intelligence directors charged with monitoring and responding to them, for the volume of activity in cyberspace and the number of ‘attacks’ is staggering.\(^43\) The constant daily assaults on governments and the industries, services, and people they guard might not constitute war in a strictly Clausewitzian sense, but they are indeed hostile, and often dangerous.

Regarding cyberspace operations as a niche on the level of international conflict should have profound if still uncertain implications for the ways in which statesmen task and organize their intelligence systems. In particular, the digital revolution may be eroding the proverbial wall between ‘operations’ and ‘intelligence’ – at least in cyberspace. Military staff charts from the early twentieth century that formally separated ‘ops’ (S-3) from intelligence (S-2) could be obsolete where collection is action and action is collection. Technology changes war and intelligence together, for the digital revolution is blurring the definition of destruction and thus of force, in that it amplifies or at least confuses the effectiveness of weapons that destroy value rather than people. If conflict is largely about being able to control and move value, and if secret means become the primary ways for guarding and taking value, then the historic closeness of war and intelligence becomes even closer.\(^44\) The digital revolution might be moving the world to the verge of

---

\(^{42}\) To cite but one example, computers in offices of the US Congress now fend off billions of ‘security events’ per year, including ‘worms, Trojan horses and spybots’. The Senate Security Operations Center alone was receiving almost 14 million attempts a day in early 2010; about four attacks per month succeeded in delivering malicious content. Erika Lovley, ‘Cyberattacks Explode in Congress’, \textit{Politico}, 5 March 2010, \url{http://www.politico.com/news/stories/0310/33987.html} (accessed 25 April 2010).

\(^{43}\) Major-General Amos Yadlin, recently noted that his nation already has an apparently parallel offensive and defensive cyberwar program, telling the Institute for National Security Studies of Tel Aviv University that ‘the cyberwarfare field fits well with the state of Israel’s defense doctrine’. Dan Williams, ‘Spymaster Sees Israel as World Cyberwar Leader’, \textit{Reuters}, 15 December 2009.

\(^{44}\) Media speculation hints that this might have already happened at the turning point of the Iraq War in 2007; see Shane Harris, ‘The Cyberwar Plan’, \textit{National Journal}, 14 November
something genuinely new, or actually very old, as the S-2/S-3 wall that was
put in place a century or more ago teeters toward collapse. At least in
cyberspace, we might be as close as anyone has ever come to Sun Tzu’s ideal
commander, who with god-like foreknowledge and cunning divines his
enemy’s plans, confounds his strategy, and renders him helpless without ever
striking him. 45

Conclusion

Technological change will continue to be comparatively rapid and profound
for the lives and institutions of people the world over. This preliminary
comparison of two intelligence revolutions might help us understand the
vector, pace, and scope of that change, and also let us glimpse how
intelligence systems might change in the future. Two particular trends bear
watching. For all intelligence systems, the digital revolution places an even
higher premium on ‘all-source’ analysis, for it is one thing to steal reams of
digital data – it is quite another to understand what in all that newly
acquired data is meaningful and important. Second, as with the race to field
and exploit machine-enciphered cryptographic systems in the twentieth
century, states and non-states that organize, task, and oversee their
intelligence officers to solve communications and security problems first
and (relatively) best will have significant advantages over those that lag
behind. These developments make the study of how states and non-states
organize and task their intelligence systems ever more important. The final
trend to anticipate under this heading is new thinking. Cyberspace is both a
level of conflict and a domain for waging it. The result so far has been
uncertainty. Intelligence systems and nations that sort out their thoughts first
and best may gain real advantage over those that lag behind.

Another issue for the foreseeable future is whether the big organizations
and large systems originally built during the Cold War will continue to
retain their advantages over the smaller upstarts. Size can be a real
disadvantage, if it makes an organization clumsy and resistant to innovation.
Then again, large organizations have their strengths as well as their
weaknesses. As Wilhelm Agrell has noted, intelligence organizations for a
range of reasons (including secrecy and mission) are among the most durable
and enduring institutions in any governmental system. 46 Large organizations
can indeed be sclerotic, but they can also afford and nurture ‘innovation.

January 2010).

45Thus, those skilled in war subdue the enemy’s army without battle. They capture his cities
without assaulting them and overthrow his state without protracted operations. Your aim
must be to take All-under-Heaven intact. Thus your troops are not worn out and your gains
will be complete. This is the art of offensive strategy.’ Sun Tzu, The Art of War, III:10-11 (as

46Professor Agrell made this comment at the conference on ‘100 Years of British Intelligence:
From Empire to Cold War to Globalisation’, Aberystwyth University, 2 May 2009.
cells' and link them together in ways that smaller intelligence systems cannot. What makes these new dilemmas more difficult for some state intelligence systems is that they are layered over the very same unresolved dilemmas that bedeviled those systems in the analog age. This is particularly acute for the nations that built the biggest collection systems. The old style of targets have not gone away, the older collection technologies still have value, and those technologies remain just as difficult to manage so as to serve national and departmental customers. Seemingly obsolete intelligence programs can rarely be simply switched off, and in the absence of major disasters will not be, because they consume significant resources and occupy people who cannot easily be sacked or shifted to new jobs. The smaller intelligence systems that never built up such capabilities in the first place may be swifter to spot opportunities and adapt to the new digital age. At any rate, organizational change is already occurring, although for the most part it has taken place within the structures of earlier organizations rather than by toppling those organizations and erecting new ones in their places.

Acknowledgements

The author is an historian with the US Department of Defense (DoD). The views expressed are those of the author alone and should in no way be interpreted as conveying official positions of the DoD or any other US government entity.
I. INTRODUCTION

A. Background

In March of 2006, journalist David Perera reported on the potential for Chinese hackers to break into the Department of Defense’s Non-classified Internet Protocol Router Net (NIPRNet), 1 the network that provides communications services among various commands and branches within the military. 2 This could be done, Perera wrote, to stifle the American response to a potential invasion of Taiwan. 3

At an Air Force Information Technology Conference just a few months later, then Major General William Lord told his audience “China has downloaded 10 to 20 terabytes of data from the NIPRNet.” 4 He suggested these attempts were aimed at acquiring data to allow hackers clandestine access to the network in the future, and called the issue “a nation-state threat by the Chinese.” 5

Cyber-espionage threats are growing. 6 According to Army General Keith 364 Alexander, Commander of U.S. Cyber Command, “DOD systems are probed by unauthorized users approximately 250,000 times an hour, over 6 million times a day.” 7 However, another estimate from Chief Information Assurance Officer for the Department of Defense Robert Lentz suggests the number is actually closer to 360 million probes per day. 8 With regard to federal government systems more generally, attacks on those systems in 2010 increased thirty-nine percent from the previous year. 9 The United States is by no means the sole target of these efforts—the United Kingdom, 10 France, 11 and South Korea 12 are among the more recent targets of cyber-espionage. Moreover, certain countries have been publicly identified as perpetrators of this conduct. 13

The threat posed by cyber-espionage will continue to develop, but debate exists as to how the United States can adequately address it. Following this introduction, the article briefly examines the cyber-espionage phenomenon with particular attention paid to major events over the last five years. The following section surveys international and U.S. law on espionage and draws on the work of scholars to suggest a less alarmist view of espionage generally. In particular, this article concludes that cyber-espionage, like any other form of espionage, is permissible under international law. The next section focuses on the consequences of espionage in the cyber domain and how, despite its notoriety, it should be recognized as a valuable tool for countries in promoting international stability. Lastly, the article reviews the tools that are at the government’s disposal in dealing with cyber-espionage, and examines proposals made by scholars to address this method of intelligence gathering.
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT..., 20 CommLaw...

*365 B. Definitions

This paper addresses cyber-espionage, also known as “cyber-exploitation,” defined by Herbert Lin as “the use of actions and operations--perhaps over an extended period of time--to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks.”

Action through cyber-exploitation is generally covert and is conducted though the least intrusive means in order to extract the sought-after information. Individuals who engage in cyber-exploitation attempt to leave undisturbed the normal operations of a computer system or network, and an ideal method is one that goes undetected by the user.

Cyber-espionage can be contrasted with other forms of cyber activities. Such activities include “cyberterrorism” or full-on “cyberwar”, both of which could have devastating effects, as compared to others that are less severe in nature, such as low-level “cybercrime” or “cybervandalism.” The technical aspects of these activities complicate the determination of whether cyberespionage is merely espionage or whether it is something more a daunting task for federal regulators and those tasked with defending our networks.

One technique that can be utilized is system probing, which consists of gathering valuable intelligence while causing no damage to the network. Dr. Herbert Lin of the National Research Council analogizes such activity to approaching a country's airspace without violating it to engage in observations from the air and to test the country's air defense response. This type of behavior alone, although typically regarded as unfriendly, would not normally raise any use of force concerns. If a method of cyber-espionage is the use of such a payload, even if it is designed not to result in any harm to the host system, the host country will not necessarily have that knowledge and could perceive the payload as a harmful threat.

Indeed, probing can be a precursor to something far more destructive, illustrated by the Russian-Georgian crisis of 2008. While there have been many more examples of pure cyber-espionage activities that have not served as staging for a subsequent attack, government and military officials must nonetheless consider the possibility that a systematic probing and incursion onto sensitive systems could be such a preparatory measure.

Dr. Lin also provides an example in which an “offensive cyber operation” deploys a dual purpose payload into the computer network of an adversary. The payload's first role is merely data observation and collection, activity that falls under the espionage category. The second role is to neutralize the system upon command. Whether the deployment of such a payload amounts to espionage or rises to the level of the threat or use of force is a difficult question to resolve.

The Stuxnet worm presents an example of the potential for this type of dual-payload system, though the worm was not employed for espionage purposes. Stuxnet first gained public attention in June of 2010 by researchers in Belarus, who observed its presence on computers belonging to their Iranian clients. Stuxnet's purpose was to disable centrifuges at the Natanz Fuel Enrichment Plan in Iran by manipulating industrial control equipment developed by Siemens. Stuxnet raises significant questions for policymakers and may represent the future of cyber operations.

C. Recent Incidents of Cyber-Espionage

In addition to the NIPRNet example above, other incidents help to illustrate exactly the range of cyber-espionage threats countries face.
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT..., 20 CommLaw...

*367 In the fall of 2007 British authorities announced that various government systems had been penetrated by hackers. The London Telegraph reported that the hackers were associated with the People's Liberation Army of China and that the hackers had targeted up to ten departments, including the Foreign Office and Home Office. 27 One expert characterized the conduct as occurring over a period of years, and that it fit within “a new doctrine of the PLA described as ‘pressure point warfare’—the attacking of specific nodes to leave the adversary paralyzed.” 28 Attempts to gain access to British government systems have continued, and have led to calls by Foreign Secretary William Hague for the adoption of “acceptable rules” for nation state behavior in the cyber realm. 29

Halfway across the world in 2008, the Indian government announced that it was the target of cyber-espionage activities. The Times of India reported that Indian systems had suffered daily breaches, allegedly by the Chinese, for over a year and a half. 30 Officials indicated that while hacking is a common occurrence, the type conducted by the Chinese was “far more sophisticated and complete,” aimed at not only gaining content from the systems but also discerning vulnerabilities for future exploitation in the event of a broader conflict. 31 The Times of India article was met with some skepticism, 32 and the Chinese government unsurprisingly denied the accusations, going so far as to suggest other countries may be using Chinese systems to carry out such attacks. 33 While many countries treat attacks like those suffered by India as “security breaches,” the Indian government considers them on par with “Internet-based terrorist attacks.” 34 India has continued to experience exfiltration of sensitive information through cyber-espionage, including data *368 related to defense systems. 35

Private industry is not immune from this type of conduct either and often presents a ripe target for cyber spies. In April of 2009, the Wall Street Journal reported that hackers were able to access computer systems containing data on the Joint Strike Fighter project, stealing “several terabytes of data related to design and electronics systems.” 36 It was suspected that computer systems used by contractors on the project had been breached over a period of years, and former officials indicated China was likely the culprit behind the intrusions. 37 That same day, however, Pentagon officials and Lockheed Martin, the affected contractor, downplayed the story, claiming that the Wall Street Journal article misrepresented the facts. 38

The following month, hackers broke into the Homeland Security Information Network, an unclassified but nevertheless sensitive data sharing system utilized by the Department of Homeland Security and state and local authorities. 39 Administrative data files—including “telephone numbers and email addresses”—were apparently the only files accessed, 40 even though this seemingly innocuous data could be used for other espionage efforts. 41

The most recent and noteworthy incident of cyber-espionage involved a major intrusion into the computer systems of the International Monetary Fund (IMF). 42 While officials’ initial statements were muted, they later disclosed that the breach was “sophisticated” and “involved significant reconnaissance prior to the attack.” 43 Investigators have since indicated that the intrusion was “linked to a foreign government,” and resulted in a major loss of data. 44

*369 These incidents demonstrate the prevalence of cyber-espionage, the wide range of information that can be stolen, and the resulting impetus on states to not only defend against these intrusions but also develop the means to conduct them. The following section provides some insight into how countries are gearing up to operate in the cyber realm.

II. CURRENT STATE OF THE LAW
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT ..., 20 COMM.LAW...

A. Sources of International Law

J.L. Brierly defined international law as "the body of rules and principles of action which are binding upon civilized states in their relations with one another." As John Perkins observed, "[I]nternational law develops in response to an inexorable logic of international relations. It is imposed by the realities of foreign policy. The roots of the law and of its legitimacy lie in this dynamic."

The Statute of the International Court of Justice provides that the court shall consider four sources to decide cases. These include treaties, "whether general or particular, establishing rules expressly recognized by the contesting states;" custom, consisting of opinio juris and general practice; "general principles of law recognized by civilized nations;" and "judicial decisions and the teachings of the most highly qualified publicists of the various nations." Given the dearth of treaties and judicial decisions on the matter of peacetime espionage, the works of learned publicists serve an important role in addressing legal issues relating to espionage.

National laws, on the other hand, largely govern the conduct of states within their internal borders. Thus, when analyzing the legality of peacetime state-sponsored cyber-espionage, it is important to recognize the dynamic between national laws and international law, and how that can influence the conduct of states.

B. International Law Regarding Cyber-Espionage

Disagreement abounds as to whether peacetime espionage is permissible under international law. Interestingly, international law has not evolved to address the finer aspects of the question--this has been the case during the height of the Cold War and even into the 21st century.

Support for the permissibility of peacetime espionage under international law extends as far back as the 17th century to the writings of Grotius, a major figure in the development of modern international law. Though espionage conducted in wartime has received attention in international law, in particular the laws governing armed conflict, peacetime espionage has not. According to Roger Scott, "[e]spionage is not prohibited by international law as a fundamentally wrongful activity; it does not violate a principle of jus cogens." A jus cogens norm is defined by the Vienna Convention on the Law of Treaties as "a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character." Consequently, a prohibition of or limitation on peacetime espionage is largely governed by the domestic laws of nations.

This view most comports with reality given the nature of statecraft and geopolitical necessities. As one scholar observed, "there has never been a war without spies, and there never has been a peace in which spies have not engaged in preparations for a future war." Espionage serves a critical purpose in enabling states to acquire information on allies and enemies alike, information that may be difficult to discover through more conventional means. This information in turn allows states to effectively navigate the rough currents of international relations and preserve their individual security.

Despite having its share of supporters, the position that peacetime espionage is illegal under international law is ultimately misguided. Professor Radsan cited Manuel Garcia Mora's claim that "peacetime espionage is regarded as an international delinquency and a violation of international law," though Mora himself acknowledged the point is thoroughly contested.
Richard Falk argued espionage is illegal, but noted there is "considerable persuasive policy available to oppose" that conclusion. 61

Quincy Wright, in a piece on espionage and aerial reconnaissance in peacetime, contended they were illegal, noting "both are illegitimate enterprises because they manifest a lack of respect for foreign territory." 62 Wright was referencing the 1960 incident in which the Soviets shot down American pilot Francis Powers as he flew over the U.S.S.R. in a U-2 spy plane. 63 Given the lack of clarity pertaining to espionage in international law, as evidenced by this incident and the related development of technologies, the 1960-61 regional meeting of the American Society of International Law ("ASIL") chose espionage as its focus. 64 Out of that meeting came a collection of writings entitled, "Essays on Espionage and International Law," which serve as the lens through which this Article examines the phenomenon of cyberespionage.

Two authors from this collection of works are Quincy Wright and Julius Stone. Called "a founding father" in the academic field of international relations, 65 Wright wrote extensively on the subject and taught for many years *372 at the University of Chicago. 66 Wright's contribution to the ASIL meeting reflected much of what he had written on the U-2 incident. He emphasized that such conduct amounted to a "violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states." 67 He further wrote, "[I]n principle, all peacetime espionage in foreign territory is illegal," conceding that "when all are engaging in it, it seems unreasonable to single out one state for utilizing a particular form of espionage, even though that form carries possibilities of hostile action going beyond espionage." 68

In contrast to Wright's conclusions, Julius Stone took a more pragmatic view of peacetime espionage under international law. Stone taught at the University of Sydney for thirty years, focusing on jurisprudence and international law, and is widely considered to have been "one of the premier legal theorists." 69 He strongly advocated for the establishment of a hotline between the governments of the U.S.S.R. and the United States during the Cold War, a tool crucial for the nuclear age as well as the cyber age. 70 With respect to this topic, Stone contested Wright's condemnation of aerial espionage during peacetime as illegal under international law, undertook his own analysis of the matter, and ultimately concluded that, absent any collateral illegality, no prohibition on peacetime espionage exists. 71

He began by positing "a view of espionage which transcends that of traditional international law," one born out of the Cold War stand-off that could benefit both sides of that divide. 72 Stone contrasted his era of technological revolution with the period over which the laws of espionage evolved, where communication was largely conducted "face to face, or by physical writing, by carriage, on foot, or on horseback." 73

Stone analyzed espionage at a time in which the world witnessed the utilization of sophisticated radio communication and satellite technology, along with high altitude surveillance aircraft. 74 He observed how this technological growth altered espionage and the types of information sought by *373 countries. 75 Stone cautioned that "our very survival now depends on being contemporaneous in our thinking, and not pretending that we can either govern or preserve ourselves in a transformed world, by the use of notions no longer applicable." 76 To that end, he recognized that espionage would evolve to depend on means such as satellite reconnaissance or sea-based surveillance, which would diminish collateral illegality like territorial intrusion. 77

Stone's underlying argument rested in the context of the Cold War. He argued that the failure to achieve an inspection regime for the United States and U.S.S.R. meant that such information needed to be acquired by some other means, and the imperfect
solution was reciprocal espionage. \textsuperscript{78} He argued that “a good system of international inspection must be basically a system of reciprocal espionage, with a seal of international umpireship on it.” \textsuperscript{79} Thus, without an officially accepted system in place, the only recourse to stave off disaster is mutually tolerated reciprocal espionage. \textsuperscript{80}

Stone conceded that this approach posed difficulties. If one were to accept his premise, a major obstacle would be distinguishing between what he termed “red light” and “green light” espionage. \textsuperscript{81} Red light espionage is the sort which “served the common-interest function” of espionage and would give warning of the spied-upon state’s preparation for an impending surprise attack. \textsuperscript{82} Green light espionage, on the other hand, serves “the divisive and destructive function” in offering the spying state knowledge that the spied-upon state was vulnerable to a first-strike, thus inviting an attack. \textsuperscript{83} Whether each country would only conduct “red light espionage” and how other states could verify this is an issue under his framework on which he did not elaborate.

Stone’s view has some modern descendants. Christopher Baker fixes espionage in functional roots, arguing that espionage facilitates state cooperation and ultimately international security. \textsuperscript{84} Baker premises his argument on the idea that treaty enforcement methods, namely verification and assurance measures, are limited in their ability to accomplish their stated purposes. \textsuperscript{85} He points to the Comprehensive Nuclear Test-Ban Treaty and how its procedure allows for states to take precautions prior to scheduled inspections and thus obscure the extent of their treaty compliance. \textsuperscript{86}

As a result, Baker sees espionage as a back-up measure of sorts for building cooperation among states. He argues that espionage allows states to “enjoy greater certainty that they will be able to validate international compliance, or at least detect when other participants are failing to comply with the treaty.” \textsuperscript{87} He suggests that espionage allows states involved in complex negotiations to better understand one another. As a result, espionage “creates a cooperative opportunity for parties with similar functional interests to negotiate mutually-beneficial outcomes.” \textsuperscript{88}

The justifications proffered by Stone and Baker offer a compelling defense of espionage under international law; however US law is not so amenable. This next section briefly discusses the status of national law on the matter.

C. U.S. Law

1. Espionage Act of 1917

Enacted following America’s entrance into World War I, \textsuperscript{89} the Espionage Act of 1917 is a far-reaching statute that Congress devised to address issues related to interference in U.S. foreign affairs and commerce, in addition to espionage. \textsuperscript{90} The Act criminalizes conduct involving the illicit acquisition of information relating to national security that is intended to either harm the United States or benefit a foreign nation. \textsuperscript{91}

According to Herbert Packer, the “legislative trend has been to increase the scope of these provisions, to provide severer penalties, and to lengthen the time within which prosecutions may be commenced.” \textsuperscript{92} Post-World War II discoveries of the extent of Soviet espionage efforts against the U.S. during the war in part prompted that legislative effort. \textsuperscript{93}

The statute’s provision on the gathering of defense information describes various methods of illicit acquisition, namely when an individual “goes upon, enters, flies over, or otherwise obtains information ....” \textsuperscript{94} The statute’s definition of defense information itself is comprehensive and covers information related to military systems and structures, civil infrastructure, and
many other items of strategic significance to the United States, in addition to virtually anything connected with "the national defense." A case brought under this law for cyber-espionage could fit under the statute's catch-all "otherwise obtains information" provision. However, given the unique characteristics of cyber-espionage, an issue regarding the application of U.S. law abroad arises.

In United States v. Zehe, a district court addressed the extraterritoriality of the Espionage Act. Zehe was an East German national accused of committing acts of espionage against the United States while in foreign countries. In its memorandum opinion, the court found that, as espionage is a crime threatening national security, it "can therefore be punished by Congress even if committed by a noncitizen outside the United States." The court noted that the statutory language did not distinguish between citizens and noncitizens, and that the crime would probably occur as often outside the United States borders as it would within. The court also found the removal of the territorial limitation on the scope of the Act indicative of Congress's intent to have the Act apply extraterritorially. The value of Zehe is unclear, and as of this Article's publication, no case involving prosecution for extra-territorial cyber-espionage under the Espionage Act has taken place or been documented.

2. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") is particularly relevant for cyber-espionage. The CFAA was first enacted in 1984, at a time when legislators did not fully grasp the scope of computer crime. With regard to espionage activities, the legislation was crafted so as "not [to] extend liability beyond existing espionage laws." The Act contains two provisions potentially applicable to cyber-espionage. The first prohibits accessing without authorization any computer, thereby acquiring sensitive information, and subsequently disseminating that information to persons unauthorized to receive it. The second provision forbids accessing without authorization a US government computer in such a way as to "affect" the use of that computer by the government. The Act also grants the Federal Bureau of Investigation primary authority to investigate crimes under (a)(1) involving espionage, indicating that cyberexploitation was a focus of the Act.

There are no indications that the CFAA has been applied extraterritorially. However, not all acts of cyber-espionage may necessarily be conducted from abroad, and the placement of a malware-infected flashdrive on an unsecured computer could yield the same result as an online cyber-espionage operation. Hence, the CFAA may allow the U.S. to prosecute some cyber-espionage, but only to a limited degree.

Having examined the international and national legal landscapes for peacetime espionage, the next section analyzes the extent to which the Stone and Baker justifications of espionage can withstand the continuing evolution of cyber-espionage.

III. CYBER EFFORTS ABROAD

In the face of these phenomena, many countries are developing cyber-capabilities to help them detect and neutralize this increasing threat.

A. China and the Koreas
The threat of Chinese cyber-espionage has been a subject of immense interest to governments and researchers alike. The Chinese military established its first cyberwarfare units in 2003, though it was not until 2010 that the Chinese unveiled what has been dubbed the “[People's Liberation Army] cyber command.” The command’s purpose is to “address potential cyber threats and to safeguard China’s national security.” Curiously, the creation of this command is aimed at strengthening China’s ability to defend its networks from intrusions and attacks.

This claim, though somewhat audacious given China’s reputation in this field, is substantiated at least in part by a recent report conducted by the Chinese technology development firm Rising. The report indicated that the United States, Japan, and South Korea bore responsibility for ninety percent of attacks on Chinese classified networks originating outside the country. Along with several related personnel changes in the upper ranks of the Chinese military, this development suggests that the cyber arena is having more influence on Chinese military strategy.

More recently, former U.S. Secretary of State Henry Kissinger issued calls for China and the United States to reach what was characterized as “cyber detente” in the face of the tremendous cyber capabilities both countries possess. Around this time, it was reported that the People's Liberation Army’s official newspaper called for the acceleration of cyberwar capability development in the face of growing U.S. military aggression on the Internet.

A week later, however, Chinese officials spoke in a much less alarmist tone, claiming that no state of “cyber war” exists between the two countries, adding that the two governments were not responsible for any hacking against either country. Given the tight control China exerts over its media, it is unclear whether such conflicting messages were the result of backtracking or strategic doublespeak, but regardless of the explanation China will continue to develop its cyber capabilities to counter any perceived threats.

The Korean peninsula has also featured a cyber element in the midst of tension between the Republic of Korea (ROK) and the Democratic People's Republic of Korea (DPRK). The DPRK’s cyber capabilities were in the spotlight back in 2009 when ROK intelligence officials indicated that the DPRK had dispatched cyber teams overseas to China to carry out operations. Though there was disagreement as to the veracity of the intelligence apparatus’ claims.

The following year, the ROK established its own “cyber command” aimed at defending against cyber threats while simultaneously developing offensive capabilities for use presumably against the DPRK. The ROK has also established various “cybersecurity centers” to help agencies defend against the threat posed by DPRK hackers, based in part on information from DPRK defectors.

B. The Middle East and India-Pakistan

Middle Eastern countries are also bolstering their cyber capabilities, though not all are doing so in the conventional sense. Israel has significant capabilities both in terms of offensive attacks as well as infiltration measures, and is even ranked as the sixth on a list of “cyberwarfare threats” by a U.S. consultancy firm. In addition to having military teams allocated to this field, the Israelis announced the creation of their own “cyber command” aimed at defending “critical computer systems.” There is widespread speculation that Israel may have been responsible for the development of Stuxnet, though no dispositive proof has been produced.
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT...; 20 CommLaw...

Iran has bolstered its capabilities in this area in the aftermath of the Stuxnet affair. The Iranians responded by undertaking a massive recruitment effort for a cyberwar force, which serves within the Iranian Revolutionary Guards. Despite Iranian rhetoric suggesting sophisticated abilities, much of their efforts in this area appear to be focused on taking down opposition websites and blogs that are critical of the current government. However, in June of 2011 an Iranian military official discussed the country's efforts in developing a cyber command to counter what it sees as growing Western incursions into its political sovereignty, what it deems "soft warfare."  

Syria has also made strides in developing offensive cyber capabilities, but those capabilities appear focused on attacking foreign websites and cracking down on domestic dissidents in the wake of the Arab Spring. Additionally, Turkey has undergone cyberattack drills aimed at assessing the government's ability to respond to such threats.

Meanwhile, cyber threats against India have led the country to begin developing its own Cyber Command & Control Authority. The centralized organ was deemed necessary, as ad-hoc responses by individual agencies were seen as ineffective in countering attacks and intrusions into government systems. The most recent cyber spats involved hackers located in India attacking Pakistani websites, ostensibly in remembrance of the victims of the Mumbai terrorist attacks of 2008, but that is arguably part of a larger underlying tension between the two countries. India has also increasingly cooperated with the United States on cybersecurity issues, with the goal of developing a peaceful and secure Internet.

Not much is known of Pakistan's cyber capabilities. Though India has been engaged with Pakistan in cyber conflict, it has largely consisted of vandalism of various websites and efforts to control other sites. However, in May 2011, the Hindustan Times reported that an officer of the Inter-Services Intelligence (ISI), Pakistan's intelligence service, hacked into an Indian Army major's email account and in the process secured "many sensitive documents." Compounding the severity of the breach was that the victim had secret and top secret documents that he was not authorized to access, multiplying the potential intelligence coup for the ISI.

**380 C. Russia and Europe**

Information on Russia's cyber-espionage institutions and doctrines is scant. Russia and the US are equally active in cyber intelligence gathering from the other, as well as keeping those cyber capabilities obscured. Russia is estimated to spend approximately $127 million on its cyberwarfare programs, with a force size of more than 7,300 personnel. The Federal Protection Service is chiefly responsible for the gathering of signals intelligence, though the Foreign Intelligence Service (SVR) and Military Intelligence (GRU) play a role in this area as well. Russia's precise capabilities in terms of cyberespionage are also unclear, but two incidents reveal a certain level of sophistication.

During the weeks prior to the Russian-Georgian conflict in 2008, Russian hackers engaged in "information exfiltration activities conducted to accumulate military and political intelligence from Georgian networks." The intelligence gathering conducted by the hackers represented a complex and highly coordinated operation, and illustrates the blurring of the lines between routine cyber-espionage and espionage as a precursor to cyber and conventional warfare.

The following year Russian "hacktivists" were accused of orchestrating an intrusion into the computer systems of the University of East Anglia's Climatic Research Unit and subsequently leaking thousands of emails incriminating scientists in a data manipulation scandal. No firm link between the act and the Russian government was established. The selection of emails and
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT ..., 20 CommLaw...

complexity of the data in question led to speculation that the incident was not one conducted by average computer hackers but likely involved in some capacity Russian intelligence. If the accusations are well-founded, this incident indicates Russia's willingness to use cyber-espionage as a means of influencing policy at the international level.

European nations have also been spurred to act in the face of this evolving threat. In 2009, the United Kingdom's government created two organizations, the Cyber Security Operations Centre (CSOC) and the Office of Cyber Security (OCS), which are tasked with analyzing trends in cyberspace and working on preventing threats against British systems. Some reports indicated that the OCS would have offensive capabilities, including "exploiting opportunities in cyber space," though officials did not explain what that meant in greater detail.

In 2009, France formed the French Network and Information Security Agency ("FNISA") to safeguard government information systems and react to cyber threats. FNISA resides under the authority of the General Secretary for National Defense, though the agency also plays a role working with the private sector in keeping cyber ahead of security threats.

Germany, in response to numerous incursions into its systems--over 1600 cyber attacks in 2010 alone--established its own National Cyber Defense Center ("NCDC") in Bonn in June 2011. With the creation of the NCDC, the newly appointed Interior Minister referred to cyber security as "a central issue." The NCDC actually comprises many agencies working together to defend against cyber threats.

The Swiss are developing an outfit for Computer Network Operations within their existing Centre for Electronic Operations of the Armed Forces Command Support Organisation ("CEO"). Swiss legal opinions preclude the use of Computer Network Exploitation for any purpose other than defensive measures, though the CEO plans to fully develop attack and exploitation capabilities.

At the intergovernmental level, the North Atlantic Treaty Organization (NATO) has also taken steps to develop cyber warfare defense, including the creation of the Cooperative Cyber Defence Center for Excellence, the mission of which is to "enhance the capability, cooperation and information sharing among NATO, NATO nations and Partners ...." Another NATO organization, the Cyber Defence Management Authority, is tasked with "coordinating cyber defence across the Alliance," and operates under the authority of the NATO Consultation, Control and Command Board. The extent to which these organizations are equipping NATO countries to conduct cyber-espionage or other activities is unclear, though defending against cyberespionage will likely factor into their efforts.

IV. UNIQUE ASPECTS PRESENTED BY CYBER

Unlike the political atmosphere of the Cold War, the current international climate is not one dominated by two superpowers with an arsenal of nuclear weapons poised for global annihilation. Rather, the means and modes of wreaking havoc are in many hands. With human rights abuses and political revolutions coming into greater importance for foreign policy, access to reliable intelligence through a variety of means is increasingly necessary. Indeed, information pertaining to allies and adversaries is even more crucial in today's environment.

Espionage—and in particular cyber-espionage—is a balance of trade-offs. States have a vested interest in having as much reliable information as possible at their disposal. That information comes at a cost, however, whether in manpower, treasure, or the potential loss of amicable relations with fellow countries. No doubt Stone and Baker raise compelling arguments supporting the
merits of espionage, in particular as it benefits international security and cooperation. But the calculus for the espionage trade-offs is altered when it takes place in the cyber domain, and whether Stone's and Baker's constructs of espionage can withstand the changes presented is another matter. There has been little scholarship on the evolution of technology and its effect on the legality of peacetime espionage. Stone and Baker thus provide a stepping stone to analyze the issues presented by cyber-espionage.

At the time Stone made his assertion, the technological frontier for espionage involved satellites, specialized aircraft and sea vessels, all of which could collect intelligence without ever crossing into the territory of another country. He also noted, with respect to the issues raised by space technology, that "territorial sovereignty in the old sense of full psychological sanctity is no longer with us." His forecast proved accurate, as the technical means put into use rapidly evolved throughout the Cold War and proved useful means for the United States to acquire intelligence.

Cyber-espionage exponentially increases those changes contemplated by Stone. The 1960 U-2 crisis was a relatively straightforward situation involving a US aircraft breaching the territorial sovereignty of the USSR, albeit for reconnaissance purposes only. The flights were motivated by a desire to respond to significant espionage effort put forth by the Soviets, who utilized both an extensive personnel network in the United States, as well as their nascent but effective satellite reconnaissance capabilities. The flights were further justified on the grounds that they were not armed and therefore not provocative in nature. Despite these considerations, their revelation still caused a massive international crisis.

The U-2 over-flights also revealed that the Soviet Union's military was much weaker than previously suggested. This knowledge arguably contributed more to stability than did reliance on less accurate means of intelligence. This is consonant with "Eisenhower's dictum that intelligence on 'what the Soviets did not have' was often as important as information on what they did."

Furthermore, the frontier of what Stone referred to when speaking of espionage that would require no collateral illegality is very nearly reached with cyber-espionage. It can be done from anywhere and often through surreptitious means. This method avoids the risks accompanied by in-person espionage or aerial over-flights.

Personnel are often put in harm's way with traditional forms of espionage, whether they are on the ground clandestinely, flying high above in an aircraft, or within foreign territory conducting maritime surveillance. With cyberespionage, the "spy" can operate from the relative safety of his or her home country, using technology as the means of acquiring intelligence. If the means employed work as intended, the spied-upon target won't know anything is amiss; if they malfunction or otherwise fail the risk of harm to the "spy" or host state is relatively minimal.

As the examples of cyber-espionage in Section I demonstrate, the acts are often traced back to servers in foreign countries—meaning the act of gathering this information is occurring outside of the target states. Additionally, an intrusion traced to a server in a particular country may nonetheless have been committed by another country, either through technical means such as routing or by physically conducting an incursion from that particular country. These measures, though not necessarily immune from investigation and attribution, can make those tasks much more difficult for the target state, as well as host countries.

Moreover, Stone's "green light espionage" can be much more problematic in the cyber realm. Lieutenant Commander Paul Walker discusses the use of "positioning of forces" in conventional warfare as a means of achieving strategic surprise over
an adversary, and explains how that concept translates into the cyber realm. Walker identifies two components of force positioning in cyberspace: 1) “exploit a vulnerability in the system in order to get inside the system” and 2) “information-based action” from within the system to facilitate broader action.

Examples of this second prong could include “altering data, destroying data, sending false messages, or causing systems to malfunction or stop working.” Walker further observes that positioning in the cyber context “will often involve peacetime access, either through remote or close means, in preparation for later actions during hostilities.”

This ambiguity is not too different from what the Soviets faced with the U-2 over-flights, or even the traditional conduct of espionage involving persons instead of technology. The aforementioned discussion between US and Soviet diplomats regarding the differences between spy planes potentially armed with weaponry and “secret agents” equipped with explosive charges demonstrates this parallel. One could point to the dual-payload pieces of code discussed by Lin and find that a threshold has been crossed, that cyber is different than anything previously encountered. After all, with some sophisticated malware, one country could secure battle plans, infrastructure schematics, and other sensitive material from an adversary, all as a prelude to a massive attack.

Such a claim is too attenuated, despite the potential for significant harm that could result from offensive cyber measures directed at the United States. While it is true that the concerns raised by Stone regarding the distinction between green light espionage and red light espionage are amplified in the cyber realm, those concerns persist with the other forms of espionage previously discussed. Spies infiltrating the country and hiding in plain sight working for sensitive facilities can commit sabotage and wreak havoc. Surveillance aircraft and reconnaissance satellites could be equipped with volatile weapons to deploy and decease the surveilled until it is too late. Yet espionage by those means persists and the international community appears to tolerate it.

Based on those analogies, cyber-espionage should not be treated any differently. The benefits to international stability and cooperation as outlined by Stone and Baker are as relevant today as they ever have been. The altered calculus can be viewed in two ways—as making the threat of harmful cyberattacks much more real, and as increasing the ease by which countries can ascertain one another’s intentions and activities. To the extent that the former threat exists, the benefits offered by the latter far exceed it.

Thus, cyber-espionage, like other forms of espionage, should persist unabated. States should respond to it as they do any other attempts to acquire sensitive information: making best efforts to secure that information, and when possible, to pursue elements operating within their territory who are facilitating the conduct of cyber-espionage. But in spite of the increased use of cyberespionage by many states, there are proposals that seek to limit its scope or use altogether.

The following section examines some of these proposals and analyzes their relative merits.

V. HOW THE U.S. CAN RESPOND

A. Continued Application of Existing Law

The Espionage Act and, more directly, the CFAA provide the legal basis to prosecute instances of cyber-espionage. However, there has been a dearth of prosecutions under these laws despite the sheer number of attacks against US government systems. Even if the current law was suitable for prosecuting instances of cyber-espionage, intelligence agencies must confront another critical issue in responding to the espionage—whether to track and gain more information about those activities, or to arrest and prosecute, and thereby close a potential source of information.
B. Development of New Law to Account For Differences in the Cyber Realm

1. Cyber Espionage Act

One proposal calls for Congress to pass a Cyber Espionage Act (CEA), which would “criminalize acts of hacking intended to disrupt American economic or military computer infrastructure, military secrets, or trade secrets.” The scope of the CEA would be limited to acts that are done for the benefit of foreign governments, and intrusions originating outside the United States would fall under the jurisdiction of the Pentagon “or a related agency.”

The CEA is premised on the idea that, although 18 U.S.C. § 1030(a) already criminalizes these types of acts, it is somehow ineffective in combating the increasing threat of cyber-espionage. The author claims that the CEA serves three critical needs: first, it would allow prosecutors to go after hackers located in the US who are operating on behalf or in support of foreign governments; second, it would be a wake-up call to the Chinese that the United States takes the threat seriously and will respond, by prosecution if possible; and third, the CEA would impose stiffer penalties than those currently provided for in section 1030.

Given that the CFAA has been largely inadequate for addressing acts of cyber-espionage committed from outside the territory of the United States, the advantage to be gained by passing the CEA is unclear. To the extent that foreign nationals are conducting cyber-espionage within US borders, the CFAA and or Espionage Act may presumably be utilized. Otherwise this proposal would amount to little more than political posturing.

C. Non-Judicial or Countermeasure Responses

1. Diplomatic Efforts and Information Sharing

Another proposal in the context of economic cyber-espionage has been to exercise diplomatic power in an effort to stem espionage. Aaron Burnstein has suggested that in order to foster an atmosphere of measured trust and transparency, nation states could informally exchange information as to what scientific and technological projects each respective country is funding and the amount of resources being devoted to those projects. The exchange of this information would promote transparency by allowing countries to verify, to some extent, that technological developments in those countries are “not cast under suspicions raised by economic espionage prosecutions in the United States.”

The proposal is not without flaws, as Burnstein acknowledges, with the most obvious one being that countries are likely unwilling to share any sensitive information with other countries. He nonetheless points to current practices of information sharing among countries as a foundation upon which some future exchange could take place. Regardless of whatever information is willingly shared, countries will always seek to access more, and through whatever means available.

If the United States is particularly troubled by an act of cyber-espionage by another country, it may still utilize many of the other tools in its possession. Given the prevalence of espionage in its multitude of forms and the adept nature of counterintelligence services, it is probable that the FBI could make an arrest under preexisting laws, or deport an operative already under surveillance, as retaliation for the cyber activities of the respective country. Alternatively, the United States government could apply diplomatic pressure in a completely unrelated area as “soft retaliation” for the perceived wrongdoing. The United States could also take a more direct approach and publicly out espionage-committing countries like China for
their activities, as the Atlantic Council’s Jason Healey suggests. These responses assume that the culprit could be readily identified.

2. Counter-Espionage

Another option available to the United States, and one it in all likelihood already engages in, is reciprocal espionage. As discussed above, espionage in many respects is the practice of nation states. Under Executive Order 12333, the National Security Agency (NSA) is tasked with the collection of “signals intelligence information and data” and is thus the primary apparatus through which the United States engages in its cyber-espionage. In addition to preexisting activities, the NSA could probe the suspected country’s computer systems as a means of responding to the conduct. Yet, depending on the nature of the information accessed, the identity of the suspected country (if the conduct can be attributed to a country), as well as other factors, no response or a very subtle response may be more appropriate than any sort of blatant reaction. The chosen response will likely depend on the message desired to be sent, if any.

D. Assessment of Options

Despite the relative merits and drawbacks of the aforementioned measures, none of them individually or even taken together will prevent cyber-espionage or encourage states to cease carrying it out. Moreover, many of these proposals are in tension with one another. The proposed CEA, were it able to yield some success at stemming espionage, would likely inspire similar laws in other countries and those nations would make best efforts to intercept and prosecute U.S. “cyber spies.” In all likelihood, the CEA or a similar piece of legislation would duplicate existing federal law and do little to address persistent cyberspionage conduct.

An information sharing proposal similar to the one suggested by Burnstein would probably not be accepted. It is in every country’s interest to preserve the integrity of information systems and the sensitive data they contain. Despite sharing that countries do for strategic and cooperative purposes, when this is done, it is done voluntarily (and therefore selectively). In the case of actual intelligence data, the information is likely sanitized, to avoid revealing the sources and methods of its collection. This is all the more true in the wake of the Wikileaks-State Department scandal in 2010, in which thousands of sensitive communiqués and documents were placed on the Internet. No matter the value of the norms that may develop in terms of international cooperation or transparency, states will continue to engage in cyber-espionage.

Although an outright information-exchange regime may not be too likely in the near-term, there is cause for hope. The governments of the United States and Russia are making efforts to ensure open channels of communication exist so as to prevent potentially harmful consequences resulting from the misreading of an incident. Such arrangements could allow for states to continue intelligence gathering activities while averting a potentially hostile response.

Reciprocal espionage likely does nothing to stop ongoing espionage committed against the United States. As demonstrated above, one difficulty of cyber-espionage is that it offers all of the benefits of traditional espionage (arguably more so, given the sheer amount of information that can be collected in a relatively short period of time) with few of the consequences attendant with “traditional modes” of intelligence collection. If countries can engage in this type of behavior with impunity, cyber-espionage is unlikely to abate in the future.

*390 VI. CONCLUSION
One principle that should inform any response in this area is that espionage, cyber or otherwise, serves valuable purposes for nation states. The costs of losing sensitive information or strategic advantages are certainly great, but having access to such information from one's adversaries is crucial to effectively operating in the international community. Because of this value, calls for haphazard action at the international level for “moratoriums” on cyber-espionage should be resisted. Efforts should focus on countermeasures, capabilities, and open lines of communication to thwart potential escalations through misunderstandings.

Cyber-espionage by its nature has fewer safeguards for the surveilled states than traditional forms of espionage. As Lin suggests, this can put states in a tense position when ascertaining the threat and identifying potential responses. If the United States seeks to reduce the pervasiveness of cyberespionage, it should focus on making its computer networks less attractive a target, thereby forcing its counterparts to engage in alternative collection measures that allow for more effective enforcement.

Footnotes

1. J.D., LL.M, August 2011. The author would like to thank his thesis advisor, Marvin Ammoni, and Maj. Erik Mudrini, USAF, for insight and feedback in the completion of this article.
2. DSIN Data Services, http://commcns.org/L31uPR.
4. Id.

14 Herbert S. Lin, Offensive Cyber Operations and the Use of Force, 4 J. NATL SECURITY L & POL’Y 63, 63 (2010).

15 Id. ("Cyberexploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of the information sought.").

16 Id. at 63-64.

17 Myriam Dunn Cavelty, Cyberwar: Concept, Status Quo, and Limitations, CTR. FOR SECURITY STUDIES, 1-2 (2010), http://comcmns.org/R2Bi8r (discussing the different categories of cyber-exploitation and the limitations involved in controlling them).

18 See Lin, supra note 14, at 79. See also Section IV, infra.

19 Id.

20 Lin addresses these and other difficult questions relating to cyber-espionage. Lin, supra note 14, at 82-84.

21 David Hollis, Cyberwar Case Study: Georgia 2008, SMALL WARS JOURNAL 4 (2011), http://comcmns.org/Im6eXB. See also discussion on Russia, infra Section III.C.

22 Christopher Bronk, Blown to Bits: China’s War in Cyberspace, August-September 2020, STRATEGIC STUDIES QUARTERLY 18 (2011), http://comcmns.org/LanaGi (discussing comprehensive cyberespionage campaign conducted prior to broader cyberattack).

23 An offensive cyber operation serves to introduce “an upgradeable software agent into an adversary system.” This agent engages in cyberexploitation and operates destructive action, such as destroying read-only memories that control the boot sequence of machines. Lin, supra note 14, at 78-79.

24 See Lin, supra note 14, at 79.


30 Indrani Bagchi, China Mounts Cyber Attacks on Indian Sites, TIMES OF INDIA (May 5, 2008), http://comcmns.org/KjIPHS.

31 Senior governmental officials publicly declare “hacking” to be a routine activity that inflicts many nations, yet they privately acknowledge the severe cyberwar threat faced by China in particular. See id.

32 Richard Steinnon, The Indian Front in the Chinese Cyber War, STEINNON ON SECURITY - NETWORK WORLD (May 6, 2008), http://comcmns.org/JNRATx (suggesting that the attacks on India were merely part of China’s global espionage efforts).
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT..., 20 CommLaw...


34 Shamshur Rabb Kahn, China’s Cyber Warfare, INSTITUTE FOR PEACE AND CONFLICT STUDIES, Article No. 2597 (June 16, 2008) available at http://commcns.org/3ylIrC.


37 Id.


40 Id.

41 Shane Harris, Chinese Spies May Have Tried to Impersonate Journalist Bruce Stokes, WASHINGTONIAN (Jan. 28, 2011), http://commcns.org/JVA7uf (discussing an incident of spear phishing).


48 Id.


50 See id. ("[T]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture." (quoting Richard A. Falk, Foreword to ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v (Roland J. Stranger ed., 1962))).

51 Geoffrey B. Demarest, Espionage in International Law, 24 DENV. J. INT’L L. & POL’Y 321, 331 (1996). See also HUGO GROTIAN, THE RIGHTS OF WAR AND PEACE, INCLUDING THE LAW OF NATURE AND OF NATIONS 331 (Cosimo, Inc. 2007) (1901) ("As the law of nations permits many things, in the manner above explained, which are not permitted by the law of nature, so it prohibits some things which the law of nature allows. Thus spies, if discovered and taken, are usually treated with the utmost
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT ...

severity. Yet there is no doubt, but the law of nations allows any one to send spies, as Moses did to the land of promise, of whom Joshua was one.


See e.g., Convention (IV) Respecting the Laws and Customs of War on Land, Annex: Regulations Concerning the Laws and Customs of War on Land art. 29-31, Oct. 18, 1907, 36 Stat. 2277. See also Dieter Fleck, Individual and State Responsibility for Intelligence Gathering, 28 MICH. J. INT'L L. 687, 689 (2007); Demarest, supra note 51, at 334-35.

Demarest, supra note 51, at 330.


Vienna Convention on the Law of Treaties art. 53, May 23, 1969, 1155 U.N.T.S. 331. To this author's knowledge, peacetime espionage has not been explicitly banned under any international judicial decisions or treaties.


Falk, supra note 58, at 45, 79-81 n.28.

Quincy Wright, Legal Aspects of the U2 Incident, 54 AM. J. INT'L L. 836, 849 (1960).

Id. at 836-37.

Falk, supra note 58, at viii.


Id. at 21.


Id.

PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT..., 20 CommLaw...

72   Id. at 31.
73   Id. at 36-37.
74   Id. at 37.
75   Id.
76   Id. at 38.
77   See Stone, supra note 71, at 34.
78   Id. at 40-41.
79   Id. at 41-42.
80   Id. at 42.
81   Id.
82   Id.
83   See Stone, supra note 71, at 42-43.
85   Id. at 1102-03.
86   Id. at 1103.
87   Id. at 1104.
88   Id. at 1106.
89   Charles Cheney Hyde, The Espionage Act, 12 AM. J. INT'L. L. 142, 142(1918).
90   Id.
92   Herbert Packer, Offenses Against the State, 339 ANNALS AM. ACAD. POL. & SOC. SCI. 77, 85 (1962).
93   Id. at 85-86.
95   Id. §793(a)-(b).
97   Id. at 198.
98   Id. at 200-01.
99   Id. at 200.
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT...,
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT... 20 CommLaw...

124 Iran to Boost Soft Power Through Establishing New Cyber Command, FARS NEWS AGENCY (June 15, 2011), http://commcons.org/JNRzPD.
126 Turkey to Conduct Cyber Attack Drills, TODAY'S ZAMAN (Jan. 21, 2011), http://commcons.org/ILfjQm.
127 Harish Gupta, As Cyber Attacks Rise, India Sets Up Central Command to Fight Back, DAILY NEWS & ANALYSIS (May 15, 2011), http://commcons.org/Jm6cXF.
128 Id.
132 Sanjib Kr Baruah, ISL Major Hacked Army Officer's Mail, HINDUSTAN TIMES (May 16, 2011), http://commcons.org/L31sXX.
133 Id.
135 Kevin Coleman, Russia's Cyber Forces, DEFENSE TECH (May 27, 2008), http://commcons.org/LWNSqs.
136 ROLAND HEICKERO, SWEDISH DEFENCE RESEARCH AGENCY EMERGING CYBER THREATS AND RUSSIAN VIEWS ON INFORMATION WARFARE AND INFORMATION OPERATIONS, 28, 34 (2010), http://commcons.org/KoyQsS.
137 David Hollis, Cyber Case Study: Georgia 2008, SMALL WARS JOURNAL 3 (Jan. 6, 2011), http://commcons.org/Kw5aOL.
138 Id.
140 Id.
144 MISSION--AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION, http://commcons.org/JyIQnL.
145 Peter Sayer, France Creates New National IT Security Agency, CIO (July 10, 2009), http://commcons.org/Ij7s4m.
PEACETIME CYBER-ESPIONAGE: A DANGEROUS BUT ..., 20 CommLaw...


147 *Id.*


149 Cavelti, *supra* note 17, at 3.

150 *Id.*

151 NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *Mission and Vision*, http://commcns.org/Kw5u0N.

152 JEFFREY HUNKER, CYBER WAR AND CYBER POWER - ISSUES FOR NATO DOCTRINE 8, 9 (2010), http://commcns.org/Lfyax.

153 John J. Kruzel, *Cybersecurity Poses Unprecedented Challenge to National Security, Lynn Says*, AMERICAN FORCES PRESS SERVICE (June 15, 2009), http://commcns.org/Jm6cXG (“Once the province of nations, the ability to destroy via cyber means now also rests in the hands of small groups and individuals: from terrorist groups to organized crime, hackers to industrial spies to foreign intelligence services,” [Deputy Secretary of Defense William Lynn] told the Center for Strategic and International Studies here.”). See also COMMISSION ON THE PREVENTION OF WEAPONS OF MASS DESTRUCTION PROLIFERATION AND TERRORISM, PREVENTION OF WMD PROLIFERATION AND TERRORISM REPORT CARD (2010), http://commcns.org/JNR0P.

154 Major Arie J. Schaap argues that despite the changes cyber presents, “at its core, it is still espionage and should be looked at differently then (sic) cyber warfare operations when attempting to establish lawful or unlawful activities under international law.” Major Arie J. Schaap, *Cyberlaw Edition: Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 141 (2009).

155 Stone, *supra* note 72, at 37, 43.

156 *Id.* at 36.


159 *Id.* at 99.

160 Maarakis, *supra* note 158, at 381.


165 Hyo-sik, *supra* note 118.


168 *Id.* at 349.

169 *Id.* at 350.

170 *Id.*

171 I contacted the Office of Intergovernmental and Public Liaison for assistance in researching this information as my personal efforts have netted few results. For instance, the Cybercrime Page for the DOJ has very few prosecutions involving the espionage provision.


174 *Id.* at 232.

175 *Id.* at 232-33.

176 *Id.* at 232-34.


178 *Id.* at 987.

179 *Id.*

180 *Id.*


182 There is precedent for the latter option, as was seen during Operation Shamshir, in which the United States rolled up an extensive network of Soviet spies operating in the U.S. under diplomatic cover. Bernard Gwertzman, *U.S. Expels 25 Soviet Diplomats; Denies Link With Daniloff Affair*, N.Y. TIMES, Sept. 18, 1986, at Al.


184 A statement by Michael Hayden suggests this is the case. Kim Zetter, *Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible*, WIRED (July 29, 2010), http://commcns.org/JNRA5W (“[w]ithout going into great detail, we're actually pretty good at [cyber-espionage], and the Chinese aren't the only ones doing this.”).


186 Kim Zetter, *Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible*, WIRED (July 29, 2010), http://commcns.org/JNRA5W.


Lin, *supra* note 14, at 84.
Domestic use of aerial drones by law enforcement likely to prompt privacy debate

By Peter Finn  
Washington Post Staff Writer  
Sunday, January 23, 2011; 12:56 AM

AUSTIN - The suspect's house, just west of this city, sat on a hilltop at the end of a steep, exposed driveway. Agents with the Texas Department of Public Safety believed the man inside had a large stash of drugs and a cache of weapons, including high-caliber rifles.

As dawn broke, a SWAT team waiting to execute a search warrant wanted a last-minute aerial sweep of the property, in part to check for unseen dangers. But there was a problem. The department's aircraft section feared that if it put up a helicopter, the suspect might try to shoot it down.

So the Texas agents did what no state or local law enforcement agency had done before in a high-risk operation: They launched a drone. A bird-size device called a Wasp floated hundreds of feet into the sky and instantly beamed live video to agents on the ground. The SWAT team stormed the house and arrested the suspect.

"The nice thing is it's covert," said Bill C. Nabors Jr., chief pilot with the Texas DPS, who in a recent interview described the 2009 operation for the first time publicly. "You don't hear it, and unless you know what you're looking for, you can't see it."

The drone technology that has revolutionized warfare in Iraq, Afghanistan and Pakistan is entering the national airspace: Unmanned aircraft are patrolling the border with Mexico, searching for missing persons over difficult terrain, flying into hurricanes to collect weather data, photographing traffic accident scenes and tracking the spread of forest fires.

But the operation outside Austin presaged what could prove to be one of the most far-reaching and potentially controversial uses of drones: as a new and relatively cheap surveillance tool in domestic law enforcement.

For now, the use of drones for high-risk operations is exceedingly rare. The Federal Aviation Administration - which controls the national airspace - requires the few police departments with drones to seek emergency approval.
Domestic use of aerial drones by law enforcement likely to prompt privacy debate

Authorization if they want to deploy one in an actual operation. Because of concerns about safety, it only occasionally grants permission.

But by 2013, the FAA expects to have formulated new rules that would allow police across the country to routinely fly lightweight, unarmed drones up to 400 feet above the ground - high enough for them to be largely invisible eyes in the sky.

Such technology could allow police to record the activities of the public below with high-resolution, infrared and thermal-imaging cameras.

One manufacturer already advertises one of its small systems as ideal for "urban monitoring." The military, often a first user of technologies that migrate to civilian life, is about to deploy a system in Afghanistan that will be able to scan an area the size of a small town. And the most sophisticated robotics use artificial intelligence to seek out and record certain kinds of suspicious activity.

But when drones come to perch in numbers over American communities, they will drive fresh debates about the boundaries of privacy. The sheer power of some of the cameras that can be mounted on them is likely to bring fresh search-and-seizure cases before the courts, and concern about the technology's potential misuse could unsettle the public.

"Drones raise the prospect of much more pervasive surveillance," said Jay Stanley, a senior policy analyst with the American Civil Liberties Union's Speech, Privacy and Technology Project. "We are not against them, absolutely. They can be a valuable tool in certain kinds of operations. But what we don't want to see is their pervasive use to watch over the American people."

The police are likely to use drones in tactical operations and to view clearly public spaces. Legal experts say they will have to obtain a warrant to spy on private homes.

As of Dec. 1, according to the FAA, there were more than 270 active authorizations for the use of dozens of kinds of drones. Approximately 35 percent of these

http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204171_pf.html
Domestic use of aerial drones by law enforcement likely to prompt privacy debate

Permissions are held by the Defense Department, 11 percent by NASA and 5 percent by the Department of Homeland Security, including permission to fly Predators on the northern and southern borders.

Other users are law enforcement agencies, including the FBI, as well as manufacturers and academic institutions.

For now, only a handful of police departments and sheriff's offices in the United States - including in Queen Anne's County, Md., Miami-Dade County, Fla., and Mesa County, Colo. - fly drones. They do so as part of pilot programs that mostly limit the use of the drones to training exercises over unpopulated areas.

Among state and local agencies, the Texas Department of Public Safety has been the most active user of drones for high-risk operations. Since the search outside Austin, Nabors said, the agency has run six operations with drones, all near the southern border, where officers conducted surveillance of drug and human traffickers.

Some police officials, as well as the manufacturers of unmanned aerial systems, have been clamoring for the FAA to allow their rapid deployment by law enforcement. They tout the technology as a tactical game-changer in scenarios such as hostage situations and high-speed chases.

Overseas, the drones have drawn interest as well. A consortium of police departments in Britain is developing plans to use them to monitor the roads, watch public events such as protests, and conduct covert urban surveillance, according to the Guardian newspaper. Senior British police officials would like the machines to be in the air in time for the 2012 Olympics in London.

"Not since the Taser has a technology promised so much for law enforcement," said Ben Miller of the Mesa County Sheriff's Office, which has used its drone, called a Draganflyer, to search for missing persons after receiving emergency authorization from the FAA.

Cost has become a big selling point. A drone system, which includes a ground operating
Domestic use of aerial drones by law enforcement likely to prompt privacy debate

computer, can cost less than $50,000. A new police helicopter can cost up to $1 million. As a consequence, fewer than 300 of the approximately 19,000 law enforcement agencies in the United States have an aviation capability.

"The cost issue is significant," said Martin Jackson, president of the Airborne Law Enforcement Association. "Once they open the airspace up [to drones], I think there will be quite a bit of demand."

The FAA is reluctant to simply open up airspace, even to small drones. The agency said it is addressing two critical questions: How will unmanned aircraft "handle communication, command and control"? And how will they "sense and avoid" other aircraft, a basic safety element in manned aviation?

Military studies suggest that drones have a much higher accident rate than manned aircraft. That is, in part, because the military is using drones in a battlefield environment. But even outside war zones, drones have slipped out of their handlers' control.

In the summer, a Navy drone, experiencing what the military called a software problem, wandered into restricted Washington airspace. Last month, a small Mexican army drone crashed into a residential yard in El Paso.

There are also regulatory issues with civilian agencies using military frequencies to operate drones, a problem that surfaced in recent months and has grounded the Texas DPS drones, which have not been flown since August.

"What level of trust do we give this technology? We just don't yet have the data," said John Allen, director of Flight Standards Service in the FAA's Office of Aviation Safety. "We are moving cautiously to keep the National Airspace System safe for all civil operations. It's the FAA's responsibility to make sure no one is harmed by [an unmanned aircraft system] in the air or on the ground."

Officials in Texas said they supported the FAA's concern about safety.

"We have 23 aircraft and 50 pilots, so I'm of
Domestic use of aerial drones by law enforcement likely to prompt privacy debate

the opinion that FAA should proceed cautiously," Nabors said.

Much of the legal framework to fly drones has been established by cases that have examined the use of manned aircraft and various technologies to conduct surveillance of both public spaces and private homes.

In a 1986 Supreme Court case, justices were asked whether a police department violated constitutional protections against illegal search and seizure after it flew a small plane above the back yard of a man suspected of growing marijuana. The court ruled that "the Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye."

In a 2001 case, however, also involving a search for marijuana, the court was more skeptical of police tactics. It ruled that an Oregon police department conducted an illegal search when it used a thermal imaging device to detect heat coming from the home of an man suspected of growing marijuana indoors.

"The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy," Justice Antonin Scalia wrote in the 2001 case.

Still, Joseph J. Vacek, a professor in the Aviation Department at the University of North Dakota who has studied the potential use of drones in law enforcement, said the main objections to the use of domestic drones will probably have little to do with the Constitution.

"Where I see the challenge is the social norm," Vacek said. "Most people are not okay with constant watching. That hover-and-stare capability used to its maximum potential will probably ruffle a lot of civic feathers."

At least one community has already balked at the prospect of unmanned aircraft.

The Houston Police Department considered participating in a pilot program to study the use of drones, including for evacuations, search and rescue, and tactical operations. In the end, it withdrew.
Domestic use of aerial drones by law enforcement likely to prompt privacy debate

A spokesman for Houston police said the department would not comment on why the program, to have been run in cooperation with the FAA, was aborted in 2007, but traffic tickets might have had something to do with it.

When KPRC-TV in Houston, which is owned by The Washington Post Co., discovered a secret drone air show for dozens of officers at a remote location 70 miles from Houston, police officials were forced to call a hasty news conference to explain their interest in the technology.

A senior officer in Houston then mentioned to reporters that drones might ultimately be used for recording traffic violations.

Federal officials said support for the program crashed.

Staff researcher Julie Tate contributed to this report.

View all comments that have been posted about this article.
Article

Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age

Laura K. Donohue†

Introduction ................................................................. 102
I. Technological Leap..................................................... 112
   A. Pre-9/11 Federal Development of Biometric Technology and Collection Systems .................. 114
   B. Post-9/11 Federal Biometric and Facial Identification Programs ........................................... 119
      1. Border Security.................................................. 121
      2. Authentication.................................................. 131
      3. Investigations and Intelligence Gathering .......... 134
      4. Military Applications ......................................... 145
      5. Interoperability............................................... 148
      6. State and Local Government .............................. 153
II. Statutory Gap ......................................................... 156
   A. Personally-Identifiable Information .................... 157
      1. Privacy Act of 1974 and Systems of Records Notice .................................................. 162
      2. Exemptions to the Privacy Act ......................... 166
      3. E-Government Act of 2002 ................................. 170
      4. Oversight and Guidance ..................................... 171

† Associate Professor of Law, Georgetown Law. Special thanks to Mary Bullard, June E. Kuhn, and Todd Venie for their research assistance. Stuart Baker, David Ball, Julie Cohen, Carrie Cordero, Jennifer Grannick, Aziz Huq, Greg Klass, Harvey Rishikof, Mike Seidman, Babak Siavoshky, and Abbe Smith provided thoughtful comments on the text. The Article further benefited from suggestions made at the Georgetown Law Faculty Workshop; the Electronic Privacy Information Center’s Privacy Coalition; the George Washington Law School-Berksley Law—Privacy Law Scholars Conference; and the University of Virginia Law National Security Law Institute. Thanks to the staff and editors of the Minnesota Law Review for their assistance and attention to detail. Thanks also to Kate Zerwas Graham, and Brennan Furness, for their assistance with bluebooking and edits. Copyright © 2012 by Laura K. Donohue.

101
INTRODUCTION

On January 23, 2012, the Supreme Court ruled that the installation and use of a Global Positioning System (GPS) device constitutes a search within the meaning of the Fourth Amendment. What might appear to be a victory for privacy advocates, however, was rooted in a concept of law that is obsolete in the face of new and emerging tracking technologies.

In United States v. Jones, the government obtained a warrant granting law enforcement officers ten days to install a GPS tracking device in a car owned by the wife of a suspected

drug dealer. On the eleventh day, agents actually installed the device—not in Washington, D.C., as required by the warrant, but in Maryland. For the next twenty-eight days, the Government tracked the vehicle, later using the information to indict the car owner’s husband, Antoine Jones, on drug trafficking conspiracy charges. Four members of the Court joined Justice Scalia in relying not on whether agents had violated Jones’s reasonable expectation of privacy—the test commonly applied to the use of electronic surveillance—but on the ancient common law of trespass.

Justice Scalia explained, “It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information.” Such an intrusion “would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.”

True. But the Bill of Rights came into effect on December 15, 1791. Two hundred and twenty years later, focusing on the physical placement of the GPS device ignores the growing body of tracking technologies that make no contact with the individual. Remote identification is the law enforcement tool of the future. GPS is only an interim step.

Consider facial recognition technology (FRT). Complex algorithms measure the size, angle, and distance between features, enabling identification based on facial characteristics. Paired with video, this technology allows governments to observe and record actions in public space and to recall this information for any number of reasons. Such remote tracking is not the equivalent of placing a tail on a suspect. It requires no suspicion of any individual; it functions as warrantless mass surveillance. It is inexpensive. It has perfect recall. And it generates terabytes of new knowledge. As the court below noted in United States v. Maynard,

2. Id. at 948–49.
3. Id. at 948.
4. Id.
5. See id. The five justices did not address whether the search was reasonable within the meaning of the Fourth Amendment. Justice Sotomayor filed a concurring opinion, as did Justice Alito, who was joined by Justices Breyer, Ginsburg, and Kagan.
7. Id.
A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.¹

This level of intrusiveness suggests something different in kind, not degree, from what has come before. It is quickly becoming more common.

Patents alone demonstrate that the technology has come of age.¹⁰ Between 1970 and 1995, the U.S. Patent Office granted fewer than 10 patents involving facial recognition.¹¹ From 1995 to 2000, it issued 20 such patents.¹² Between 2001 and 2011, the number leapt to 633.¹³

These patents are increasingly focused on, and applicable to, law enforcement and national security, where applications range from confirming targets for elimination and pairing photographs and data from different databases, to monitoring individuals as they move through public space. Between 1970 and 1995, none of the patents specifically focused on law enforcement or national security. Of the patents issued between 1995 and 2000, less than half were directed at such uses. But following 9/11, three major facial recognition patent clusters with direct law enforcement and national security applications emerged: digital video (80 patents), image surveillance (35) and biometric identification data (136). (See Figure 1).¹⁴

---


11. The timing and frequency of patents was ascertained by the author by conducting structured searches of restricted time intervals in a patent search engine. See PRIORIP, http://www.prior-ip.com (last visited Sept. 18, 2012).

12. See supra note 11.

13. The number of FRT patents issued per year is as follows: 1995 (2); 1996 (2); 1997 (0); 1998 (7); 1999 (3); 2000 (6); 2001 (4); 2002 (12); 2003 (30); 2004 (17); 2005 (10); 2006 (87); 2007 (87); 2008 (30); 2009 (100); 2010 (167); 2011 (89). See supra note 11.

14. See supra note 11.
Further examination demonstrates a growing government market in this area. Major defense contractors such as Lock-
heed Martin and Honeywell International, together with myriad startups dedicated to FRT and video technologies, have swiftly moved into related technologies. Simultaneously, government agencies, such as the Central Intelligence Agency (CIA), the Defense Advanced Research Projects Agency, the Air Force Research Laboratory (DARPA), and the National Geospatial-Intelligence Agency, have invested in advanced technologies that range from behavior recognition, motion pattern learning, and anomaly detection, to object recognition and tracking.  

Government forays into biometric identification abound. The Federal Bureau of Investigation (FBI), for example, is currently developing what it calls Next Generation Identification (NGI). One of its components, the Interstate Photo System, al-


lows law enforcement to submit still images or video surveillance feeds obtained from any public or private source.\(^{18}\) The system is designed to store this data and, using FRT, to identify individuals, pairing images with biographic information.\(^ {13}\) NGI also uses biographic information to search its Repository for Individuals of Special Concern.\(^ {20}\) This database consists of records of "known or appropriately suspected terrorists," as well as "other persons of special interest" (a category that remains undefined).\(^ {21}\) NGI further includes a Rap Back Service, where employers can collect employees' biometric data and give it to the FBI, which will then notify them of any criminal, and, in some cases, civil activities.\(^ {22}\) This means that everything from criminal convictions to parking tickets to attendance at political rallies, captured on film, could be reported.

The FBI is not alone. In 2004, the Department of Defense's (DoD) Automated Biometric Identification System (ABIS), designed to work with the FBI's biometric database, became op-
erational. By 2009, DoD's database had evolved into the Next Generation ABIS, a system that combines fingerprint, palm print, facial recognition, and iris analysis with biographic and encounter transactions. It stores, retrieves, and searches data collected from "persons of national security interest." DoD has complemented this initiative with a Biometrically-Enabled Watchlist. The Department of Homeland Security (DHS) and the State Department also maintain biometric databases and watchlists. Memoranda of understanding between the agencies focus on how to make these systems interoperable.

Despite the explosion of federal initiatives in this area, Congress has been virtually silent on the many current and potential uses of FRT and related technologies. No laws directly address facial recognition—much less the pairing of facial


2012] REMOTE BIOMETRIC IDENTIFICATION

recognition with video surveillance—in either the criminal law or foreign intelligence realm. Many of the existing limits placed on the collection of personally identifiable information do not apply. Only a handful of hearings has even questioned the use of biometrics in the national security or law enforcement context.\textsuperscript{30}

The absence of a statutory framework is a cause for significant concern. Facial recognition represents the first of a series of next generation biometrics, such as hand geometry, iris, vascular patterns, hormones, and gait, which, when paired with surveillance of public space, give rise to unique and novel questions of law and policy.\textsuperscript{31} These constitute what can be considered Remote Biometric Identification (RBI). That is, they give the government the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner. As such, RBI technologies present capabilities significantly different from that which the government has held at any point in U.S. history.

Hitherto, identification techniques centered on what might be called Immediate Biometric Identification (IBI)—or the use of biometrics to determine identity at the point of arrest, following conviction, or in conjunction with access to secure facilities. Fingerprint is the most obvious example of IBI, although more recent forays into palm prints fall within this class. DNA technologies that require individuals to provide saliva, skin, or other samples for analysis also can be considered as part of IBI. Use of technology for IBI, in contrast to RBI, tends to be focused (1) on a single individual; (2) close-up; (3) in relation either to custodial detention or in the context of a specific physical area related to government activity; (4) in a manner often

\textsuperscript{30} For a notable exception, see Hearing on Oversight of the Federal Bureau of Investigation Before the S. Judiciary Comm., 110th Cong. 92 (2008) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary) ("Recent reports suggest that the FBI is engaged in a $1 billion program to create a massive biometric database, compiling not just fingerprints, but eye scans, palm prints, facial features, and other identifying features of millions of people. It is vitally important for the FBI to master emerging and enhanced technologies in the fight against crime and terrorism. But we must also be cognizant of the impact that such a database can have on the privacy rights and civil liberties of Americans.").

involving notice and often consent, and (5) is a one-time or limited occurrence. The types of legal and policy questions raised by RBI differ from those accompanying IBI.

What we are witnessing, as a result of the expansion from IBI to RBI, is a sea change in how we think about individuals in public space. Congress has yet to grapple with the consequences.

This Article seeks to drive the discussion forward by detailing the recent explosion of federal initiatives in biometric identification, highlighting gaps in the current statutory framework governing RBI, and considering the Court's jurisprudence in relation to the constitutional questions that arise. Arguing that the current statutory and constitutional framing is inadequate to address the new conditions that accompany these emerging technologies, it calls for immediate and careful congressional consideration of remote biometric identification.

Part I begins with a discussion of the evolution of biometric technologies and federal programs. Prior to September 11, 2001, there were relatively few initiatives focused on the collection and use of biometrics. Immediately following the attacks, resources flowed to this area. Initially, most of the attention centered on U.S. borders. Over the next decade, the patterns shifted. Paralleling the evolution of applications related to homeland security came efforts to expand biometrics to government employees. Traditional law enforcement collection of fingerprints expanded to include other forms of biometric data. Similar systems worked their way into the military infrastructure, with soldiers using new tools for targeting, identification, and surveillance purposes. New technologies began to extend horizontally, across federal agencies, as well as vertically, to state and local governments. Emphasis is now moving beyond merely establishing biometric systems to facilitating information sharing between these databases, blurring the line between investigations and intelligence gathering.

Part II considers the statutory frameworks that potentially apply to the current systems: government acquisition of individually identifiable data, criminal warrant requirements, and foreign intelligence surveillance. In relation to the first, federal

32. An important exception here would be the lifting of prints or collection of DNA from a crime scene, where neither consent nor notice would be present; such a scenario, however, is contemplated in the context of (3)—i.e., a limited geographic area related to government activity, in this case the investigation of a crime.
agencies have considerable, largely unchallenged authority to collect and analyze personally identifiable information. Congressional restrictions on the exercise of such authorities generally do not apply to biometric systems. Gaps in the 1974 Privacy Act and its amendments and the 1990 Computer Matching and Privacy Protection Amendments, in conjunction with Privacy Act exemptions and the 2002 E-Government Act, minimize the extent to which such instruments can be brought to bear. The second area turns on Title III of the 1968 Omnibus Crime Control and Safe Streets Act and Title I of the 1986 Electronic Communications Privacy Act. Neither statute, however, directly addresses RBI. The third area, controlled by the 1978 Foreign Intelligence Surveillance Act (FISA) and its amendments, similarly falls short. It is unclear whether biometric surveillance is considered as within the Foreign Intelligence Court’s remit. Even if it is, significant questions exist as to whether FISA’s provisions can be met by RBI. In the absence of a statutory framework with which to evaluate the current federal initiatives and their potential inclusion of facial recognition and video technologies, we are driven back upon constitutional considerations.

Part III recognizes that RBI sits uneasily in the Court’s Fourth Amendment jurisprudence, which has yet to squarely address the implications of these new technologies. Potentially applicable lines of cases depend upon conditions that fail to provide meaningful distinctions within RBI.

Part IV notes that little relief may be found in associated constitutional doctrines. The Fifth Amendment’s right against self-incrimination, understood as protecting individuals from being forced to take action, fails to reach the passive nature of ubiquitous surveillance. The First Amendment’s protection of speech and assembly present a low bar, even where RBI may be directly targeting political rallies. The Fifth and Fourteenth Amendments’ due process protections key in on the accuracy of the technology—something that may become less of an issue as research advances.

Part V concludes with the recognition that the types of questions posed by this technology may require a new approach to the place of privacy in society. Instead of focusing on the rights discourse as a framing for personally-identifiable information, it may be more important to think about privacy in a constitutive sense—i.e., as playing a role in social cohesion and personal and social development. Simultaneously, ways of iden-
tifying the technologies thus implicated, and of understanding their impact, need to be developed—this, in juxtaposition to the unmitigated embrace of new and emerging technologies and the assumption that such advances represent something merely different in degree, not kind, from what has come before.

I. TECHNOLOGICAL LEAP

For more than a century, U.S. law enforcement agencies have employed biometric identification. Such technologies initially took the form of fingerprinting. In the early twentieth century, the New York Police Department, the New York State Prison System, and the Federal Bureau of Prisons became the first to adopt this technique. Soon thereafter, the U.S. Army found a parallel use in the national security realm. In 1907, fingerprinting spread to the U.S. Navy and the following year to the U.S. Marine Corps (USMC). The use of fingerprints proved labor intensive, requiring numerous people and hours to

33. In 1892, Sir Francis Galton published his famous treatise, Finger Prints, establishing their individuality and permanence and offering the first classification system to distinguish between persons. Laura A. Hutchins, Systems of Friction Ridge Classification, in The Fingerprint Sourcebook 5-1, 5-6 (Alan McRoberts ed., 2011), available at https://www.ncjrs.gov/pdffiles1/ny/226329.pdf. Edward Hubert Henry followed Galton’s work with his Classification and Uses of Finger Prints, providing a more easily searchable system with straightforward methods of classification and comparison. EDWARD RICHARD HENRY, CLASSIFICATION AND USES OF FINGER PRINTS 3–14 (1905) (discussing Galton’s work and noting the degree to which fingerprinting had become integrated into military and civil functions in India). These studies, together with growing interest in the topic, prompted the British Home Office to conduct an inquiry into the identification of criminals by measurement and fingerprints. History of the Metropolitan Police, METROPOLITAN POLICE, http://www.met.police.uk/history/fingerprints.htm (last visited Sept. 18, 2012). By 1901 New Scotland Yard had launched its first Fingerprint Branch, adopting Henry’s system of classification. Id.


35. See id.

identify, catalogue, and compare prints stored on paper. Starting in the 1960s, the introduction of automated technology for comparison and storage altered the landscape—complex analyses could be completed within seconds. Digitization further sped the number of records that could be stored and analyzed.

By the end of the twentieth century, automated fingerprint matching had become the norm and new forms of biometric identification had begun to emerge. The government launched a number of initiatives aimed at taking advantage of the new technologies. The National Institute of Standards and Technology and the Biometric Consortium (established in 1992) created an interagency body to consider and coordinate biometric activities at the federal level. Most of the programs emphasized fingerprint and DNA as methods of identification, with further interest in facial recognition and iris analysis. Accordingly, the FBI established its Integrated Automated Fingerprint Identification System (IAFIS), while the Immigration and Naturalization Service (INS) initiated an automated biometric identification system called IDENT. The FBI also created the Combined DNA Index System, known as CODIS, a computer database that integrates local, state, and federal DNA records of convicted offenders, evidence collected from crime scenes, and missing persons.

Following the attacks of 9/11, renewed interest in biomet-


11.pdf (dating research conducted by the FBI and NIST on the automated matching of fingerprints to 1967).
41. See id. at 8. In 1998, the Immigration and Naturalization Service launched INSPASS, a system based on hand geometry, used to facilitate swifter processing of business travelers registered for the program. Id. In 1995, there was a commercial release of iris prototypes. Id. In 1996, INS launched a fully automated Port of Entry at Scobey, Montana, relying upon voice verification technology. Id.
42. See id.
rics led to an expansion of the existing databases, the institution of new programs, and the creation of new inter-agency agreements to allow for the sharing of biometric data.\(^{44}\) Like the civilian institutions, the military vigorously pursued new uses of biometric technologies, creating in the process its own database known as the Automated Biometric Identification System, with further expansion resulting in the creation of Next Generation ABIS.\(^{45}\) Federal initiatives reached beyond horizontal coordination, to include vertical integration with state and local government.\(^{46}\)

### A. PRE-9/11 FEDERAL DEVELOPMENT OF BIOMETRIC TECHNOLOGY AND COLLECTION SYSTEMS

Two federal fingerprint repositories and one DNA database predated the September 11, 2001 attacks. A brief discussion of each helps to illustrate the changed circumstances that followed.

The first initiative stemmed from research jointly sponsored in 1967 by the FBI and the National Institute of Standards and Technology.\(^{47}\) More than a quarter of a century later, the FBI began planning development of IAFIS, which became operational in 1999.\(^{48}\) IAFIS collected ten-print images, entered by local, state, and federal law enforcement agencies.\(^{49}\) It quickly came to serve as a national repository, allowing officials to check new prints against the database, and to correlate the prints to individual identity.\(^{50}\)

Throughout the 1990s, talks between the FBI and INS as to whether the latter could use IAFIS for border security exposed schisms in the agencies’ needs.\(^{51}\) INS, which was develop-

---

\(^{44}\) See BIOMETRICS IN GOVERNMENT POST-9/11, supra note 38, at 29, 26.

\(^{45}\) See id. at 25.

\(^{46}\) See id. at 29 (describing coordination of US-VISIT service amongst federal, state, and local agencies).


\(^{48}\) BIOMETRICS IN GOVERNMENT POST-9/11, supra note 38, at 8–9.


\(^{50}\) See id.

\(^{51}\) See U.S. Dept' of Justice, Status of IDENT/IAFIS Integration: Integra-
ing its own automated biometric system, emphasized the importance of being able to process a high volume of inquiries swiftly. The movement of large numbers of people and limited facilities for holding individuals at points of entry made it difficult to accommodate delays. With its operational mission in mind, INS considered two fingerprints sufficient for screening those entering and leaving the country. The FBI, in contrast, with an eye towards criminal prosecution, emphasized the importance of obtaining ten prints. The inclusion of such information, however, made searches more complex which, correspondingly, took longer.

To accommodate the special needs presented by the border, in 1994 Congress approved INS’s own repository, known as IDENT. Two years later Congress authorized further development of the integrated entry and exit data system. This database included photographs and two index finger fingerprints, with additional information related to the individual’s criminal history.

Efforts to integrate IAFIS and IDENT’s parallel fingerprint systems repeatedly stalled on the shoals of institutional needs and bureaucratic politics. In 1998, for instance, Congressman Alan Mollohan, the ranking member of the House Appropriations Subcommittee for Commerce, Justice, State, and the Judiciary, wrote to Attorney General Janet Reno, asking straight out whether the two systems were redundant.

---

52. See id.
53. See id.
54. See id.
55. See id.
56. See id.
59. See STATUS OF IDENT/IAFIS, supra note 51; see also BIOMETRICS IN GOVERNMENT POST-9/11, supra note 38, at 8.
60. STATUS OF IDENT/IAFIS, supra note 51.
Living Under Drones
Death, Injury, and Trauma to Civilians
From US Drone Practices in Pakistan

http://livingunderdrones.org/
Cover Photo: Roof of the home of Faheem Qureshi, a then 14-year old victim of a January 23, 2009 drone strike (the first during President Obama’s administration), in Zeraki, North Waziristan, Pakistan. Photo supplied by Faheem Qureshi to our research team.

Suggested Citation:

International Human Rights and Conflict Resolution Clinic (Stanford Law School) and Global Justice Clinic (NYU School of Law), Living Under Drones: Death, Injury, and Trauma to Civilians From US Drone Practices in Pakistan (September, 2012)
# TABLE OF CONTENTS

**ACKNOWLEDGMENTS** | I
--- | ---
**ABOUT THE AUTHORS** | III
**EXECUTIVE SUMMARY AND RECOMMENDATIONS** | V
**INTRODUCTION** | 1
  - METHODOLOGY | 2
  - CHALLENGES | 4
**CHAPTER 1: BACKGROUND AND CONTEXT** | 7
  - DRONES: AN OVERVIEW | 8
  - DRONES AND TARGETED KILLING AS A RESPONSE TO 9/11 | 10
  - PRESIDENT OBAMA’S ESCALATION OF THE DRONE PROGRAM | 12
    - “PERSONALITY STRIKES” AND SO-CALLED “SIGNATURE STRIKES” | 12
    - WHO MAKES THE CALL? | 13
  - PAKISTAN’S DIVIDED ROLE | 15
  - CONFLICT, ARMED NON-STATE GROUPS, AND MILITARY FORCES IN NORTHWEST PAKISTAN | 17
  - UNDERSTANDING THE TARGET: FATA IN CONTEXT | 20
    - PASHTUN CULTURE AND SOCIAL NORMS | 22
    - GOVERNANCE | 23
    - ECONOMY AND HOUSEHOLDS | 25
    - ACCESSING FATA | 26
**CHAPTER 2: NUMBERS** | 29
  - TERMINOLOGY | 30
  - UNDERREPORTING OF CIVILIAN CASUALTIES BY US GOVERNMENT SOURCES | 32
  - CONFLICTING MEDIA REPORTS | 35
  - OTHER CONSIDERATIONS THAT MAY LEAD TO CONFLICTING REPORTS | 40
    - LIMITED FIRST-HAND KNOWLEDGE | 40
    - UNREPORTED STRIKES | 40
  - STRIKE DATA AGGREGATORS | 43
    - THE LONG WAR JOURNAL | 45
    - NEW AMERICA FOUNDATION | 47
    - THE BUREAU OF INVESTIGATIVE JOURNALISM | 53
### Chapter 3: Living Under Drones

**Voices from Below: Accounts of Three Drone Strikes**
- March 17, 2011
- June 15, 2011
- January 23, 2009

**Beyond Killing: Civilian Impacts of US Drone Strike Practices**
- Impacts on Willingness to Rescue Victims and Provide Medical Assistance
- Direct Property Damage and Economic Hardship Impacts
- Mental Health Impacts of Drone Strikes and the Presence of Drones
- Impacts on Education Opportunities
- Impacts on Burial Traditions and Willingness to Attend Funerals
- Impacts on Economic, Social, and Cultural Activities
- Impacts on Community Trust

### Chapter 4: Legal Analysis

- Whether the US Use of Force in Pakistan Violates Pakistan’s Sovereignty
- Circumstances in Which Individuals May Lawfully Be Lethally Targeted
  - The Existence of an Armed Conflict in Pakistan
  - Drone Strikes under International Humanitarian Law
  - In the Absence of Armed Conflict, Only International Human Rights Law Applies
- US Domestic Law
- Accountability and Transparency

### Chapter 5: Strategic Considerations

- Drone Strike Accuracy and Effectiveness in Hampering Armed Violence
- US Drone Strike Policies Foment Anti-American Sentiment and May Aid Recruitment to Armed Non-State Actors
- Drones Undermine US Credibility in Pakistan and Throughout the Region

### Appendix A: Testimony

### Appendix B: Strike & Minimum Casualty Numbers Per Week (2010-2012)

### Appendix C: US Statements on Civilian Casualties
ACKNOWLEDGMENTS

This report is the result of nine months of research by the International Human Rights and Conflict Resolution Clinic of Stanford Law School (Stanford Clinic) and the Global Justice Clinic at New York University School of Law (NYU Clinic). Professor James Cavallaro and Clinical Lecturer Stephan Sonnenberg led the Stanford Clinic team; Professor Sarah Knuckey led the NYU Clinic team. Adelina Acuña, Mohammad M. Ali, Anjali Deshmukh, Jennifer Gibson, Jennifer Ingram, Dimitri Phillips, Wendy Sarkin, and Omar Shakir were the student research team at Stanford; Christopher Holland was the student researcher from NYU. Supervisors Cavallaro, Sonnenberg, and Knuckey, as well as student researchers Acuña, Ali, Deshmukh, Gibson, Sarkin, and Shakir participated in the fact-finding investigations to Pakistan.

In December 2011, Reprieve, a charity based in the United Kingdom, contacted the Stanford Clinic to ask whether it would be interested in conducting independent investigations into whether, and to what extent, drone strikes in Pakistan conformed to international law and caused harm and/or injury to civilians. The Stanford Clinic agreed to undertake independent fact-finding and analysis on these questions, as well as others related to drone strikes and targeted killings in Pakistan, beginning in December 2011. Later, the NYU Clinic agreed to join the research project and participated in the second research trip to Pakistan, as well as in additional research, writing, and editing of this report.

In the course of the research, the Stanford and NYU Clinics have exchanged information and logistical support with Reprieve and its partner organization in Pakistan, the Foundation for Fundamental Rights (FFR). The latter organization assisted in contacting many of the potential interviewees, particularly those who reside in North Waziristan, and in the difficult work of arranging interviews. The Stanford and NYU Clinics designed the research project, analyzed information, and drafted and edited the report independently from Reprieve and FFR.

Cavallaro, Knuckey, and Sonnenberg supervised and directed the preparation of the report, oversaw the writing, and served as the final editors of this publication. Students Acuña, Ali, Deshmukh, Gibson, and Shakir drafted initial sections of the report. Acuña, Ali, Gibson and Shakir synthesized and restructured the initial draft sections. Holland from the NYU Clinic also assisted with research for the report. Firas Abuzeid, Jennifer Ingram, Usman Liaqat, Clara Long, Waqas Mustafeez, Ada Sheng, and Zade Shakir assisted the research team in the review and fact-checking of the final version.

Abdulrasheed Alabi, Danny Auron, Dr. Rajaie Batniji, Kristen DeRemer, Aisha Ghani, Emi MacLean, Veerle Openghaffen, Professor Margaret Satterthwaite, Dr. Saad Shakir,
Hina Shamsi, Professor Shirin Sinnar, Professor Allen Weiner, and Nate Wessler reviewed and commented on this report or some part thereof. The Stanford and NYU Clinics would like to thank these scholars and practitioners for volunteering their time and expertise. The opinions and positions articulated in this report are the exclusive responsibility of the research team and not of these external reviewers.

The Clinics also extend our appreciation to the Brave New Foundation, in particular its president, Robert Greenwald, as well as Josh Busch, Aminta Goyel, Jeff Cole, David Fisher, Joseph Suzuki, and John Amick for preparing a short video to accompany the report.

The Stanford and NYU Clinics express our sincere thanks to our translators in Islamabad and Peshawar. In particular, we would like to thank Muhammad Abdullah Ather, Rascim Khan Khattak, Muzafar Mohiuddin, Obaid Khan, Adnan Wazir, Usama Khilji, and Amna Bilal.

A particular debt of gratitude is owed to those who agreed to be interviewed for this report, often at risk to themselves. This includes in particular the Waziris who traveled long distances and faced significant risks to share their accounts of living under drones with our research team.
ABOUT THE AUTHORS

Stanford International Human Rights and Conflict Resolution Clinic  
(IHRCRC)

The Stanford International Human Rights and Conflict Resolution Clinic (Stanford Clinic) addresses a range of situations of rights abuse and violent conflict around the world. By providing direct representation to victims and by working with communities that have suffered or face potential abuse, the Clinic seeks both to train advocates and advance the cause of human rights and global justice. The Clinic engages students in sophisticated and multi-disciplinary advocacy to advance the basic human rights and dignity of victimized individuals and communities globally. Students divide their time between an intensive clinical seminar and ongoing clinical advocacy projects. They are exposed to a range of tools and strategies to promote respect for rights and dignity, including factual documentation, elaboration, and distribution of reports on rights abuse, litigation before national and international institutions, community empowerment strategies, and conflict transformation techniques.

Global Justice Clinic (GJC) at NYU School of Law

The Global Justice Clinic (NYU Clinic) at NYU School of Law provides high quality, professional human rights lawyering services to individual clients and non-governmental and inter-governmental organizations, partnering with groups based in the United States and abroad, or undertaking its own projects. Serving as legal advisers, counsel, co-counsel, or advocacy partners, Clinic students work side-by-side with human rights activists from around the world. Clinic work has addressed economic and social rights; human rights, national security, and counter-terrorism; transnational corporate accountability; weapons development; and the human rights of marginalized groups. These projects give students an opportunity to assist in formulating policy, research, and legal responses to cross-border human rights problems.
EXECUTIVE SUMMARY AND RECOMMENDATIONS

In the United States, the dominant narrative about the use of drones in Pakistan is of a surgically precise and effective tool that makes the US safer by enabling “targeted killing” of terrorists, with minimal downsides or collateral impacts.\(^1\)

This narrative is false.

Following nine months of intensive research—including two investigations in Pakistan, more than 130 interviews with victims, witnesses, and experts, and review of thousands of pages of documentation and media reporting—this report presents evidence of the damaging and counterproductive effects of current US drone strike policies. Based on extensive interviews with Pakistanis living in the regions directly affected, as well as humanitarian and medical workers, this report provides new and firsthand testimony about the negative impacts US policies are having on the civilians living under drones.

Real threats to US security and to Pakistani civilians exist in the Pakistani border areas now targeted by drones. It is crucial that the US be able to protect itself from terrorist threats, and that the great harm caused by terrorists to Pakistani civilians be addressed. However, in light of significant evidence of harmful impacts to Pakistani civilians and to US interests, current policies to address terrorism through targeted killings and drone strikes must be carefully re-evaluated.

It is essential that public debate about US policies take the negative effects of current policies into account.

---

First, while civilian casualties are rarely acknowledged by the US government, there is significant evidence that US drone strikes have **injured and killed civilians**. In public statements, the US states that there have been “no” or “single digit” civilian casualties."² It is difficult to obtain data on strike casualties because of US efforts to shield the drone program from democratic accountability, compounded by the obstacles to independent investigation of strikes in North Waziristan. The best currently available public aggregate data on drone strikes are provided by The Bureau of Investigative Journalism (TBIJ), an independent journalist organization. TBIJ reports that from June 2004 through mid-September 2012, available data indicate that drone strikes killed 2,562-3,325 people in Pakistan, of whom 474-881 were civilians, including 176 children.

- The Bureau of Investigative Journalism

reports that these strikes also injured an additional 1,228-1,362 individuals. Where media accounts do report civilian casualties, rarely is any information provided about the victims or the communities they leave behind. This report includes the harrowing narratives of many survivors, witnesses, and family members who provided evidence of civilian injuries and deaths in drone strikes to our research team. It also presents detailed accounts of three separate strikes, for which there is evidence of civilian deaths and injuries, including a March 2011 strike on a meeting of tribal elders that killed some 40 individuals.

---

² See Obama Administration Counterterrorism Strategy (C-Span television broadcast June 29, 2011), http://www.c-spanvideo.org/program/AdministrationCo; see also Strategic Considerations, infra Chapter 5: Strategic Considerations; Contradictions Chart, infra Appendix C.

Second, US drone strike policies cause considerable and under-accounted-for harm to the daily lives of ordinary civilians, beyond death and physical injury. Drones hover twenty-four hours a day over communities in northwest Pakistan, striking homes, vehicles, and public spaces without warning. Their presence terrorizes men, women, and children, giving rise to anxiety and psychological trauma among civilian communities. Those living under drones have to face the constant worry that a deadly strike may be fired at any moment, and the knowledge that they are powerless to protect themselves. These fears have affected behavior. The US practice of striking one area multiple times, and evidence that it has killed rescuers, makes both community members and humanitarian workers afraid or unwilling to assist injured victims. Some community members shy away from gathering in groups, including important tribal dispute-resolution bodies, out of fear that they may attract the attention of drone operators. Some parents choose to keep their children home, and children injured or traumatized by strikes have dropped out of school. Waziris told our researchers that the strikes have undermined cultural and religious practices related to burial, and made family members afraid to attend funerals. In addition, families who lost loved ones or their homes in drone strikes now struggle to support themselves.

Third, publicly available evidence that the strikes have made the US safer overall is ambiguous at best. The strikes have certainly killed alleged combatants and disrupted armed actor networks. However, serious concerns about the efficacy and counter-productive nature of drone strikes have been raised. The number of “high-level” targets killed as a percentage of total casualties is extremely low—estimated at just 2%.4 Furthermore, evidence suggests that US strikes have facilitated recruitment to violent non-state armed groups, and motivated further violent attacks. As the New York Times has reported, “drones have replaced Guantánamo as the recruiting tool of choice for

---

militants.\textsuperscript{5} Drone strikes have also soured many Pakistanis on cooperation with the US and undermined US-Pakistani relations. One major study shows that 74% of Pakistanis now consider the US an enemy.\textsuperscript{6}

The number of “high-level” targets killed as a percentage of total casualties is extremely low—estimated at just 2%.

\textit{Peter Bergen & Megan Braun, CNN}

Fourth, current US targeted killings and drone strike practices undermine respect for the rule of law and international legal protections and may set dangerous precedents. This report casts doubt on the legality of strikes on individuals or groups not linked to the terrorist attacks of September 11, 2011, and who do not pose imminent threats to the US. The US government’s failure to ensure basic transparency and accountability in its targeted killing policies, to provide necessary details about its targeted killing program, or adequately to set out the legal factors involved in decisions to strike hinders necessary democratic debate about a key aspect of US foreign and national security policy. US practices may also facilitate recourse to lethal force around the globe by establishing dangerous precedents for other governments. As drone manufacturers and officials successfully reduce export control barriers, and as more countries develop lethal drone technologies, these risks increase.

\textbf{In light of these concerns, this report recommends that the US conduct a fundamental re-evaluation of current targeted killing practices, taking into account all available evidence, the concerns of various stakeholders, and the short and long-term costs and benefits.} A significant rethinking of current US targeted killing and drone strike policies is long overdue. US policy-makers, and the American public, cannot continue to ignore evidence of the civilian harm and counterproductive impacts of US targeted killings and drone strikes in Pakistan.


This report also supports and reiterates the calls consistently made by rights groups and others for legality, accountability, and transparency in US drone strike policies:

➢ The US should fulfill its international obligations with respect to accountability and transparency, and ensure proper democratic debate about key policies. The US should:

• **Release the US Department of Justice memoranda** outlining the legal basis for US targeted killing in Pakistan;

• **Make public critical information concerning US drone strike policies**, including as previously and repeatedly requested by various groups and officials: the targeting criteria for so-called “signature” strikes; the mechanisms in place to ensure that targeting complies with international law; which laws are being applied; the nature of investigations into civilian death and injury; and mechanisms in place to track, analyze and publicly recognize civilian casualties;

• **Ensure independent investigations** into drone strike deaths, consistent with the call made by Ben Emmerson, UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism in August 2012;

---


8 Letter from Amnesty International et al., supra note 7.

• In conjunction with robust investigations and, where appropriate, prosecutions, establish compensation programs for civilians harmed by US strikes in Pakistan.

➢ The US should fulfill its international humanitarian and human rights law obligations with respect to the use of force, including by not using lethal force against individuals who are not members of armed groups with whom the US is in an armed conflict, or otherwise against individuals not posing an imminent threat to life. This includes not double-striking targets as first responders arrive.

• Journalists and media outlets should cease the common practice of referring simply to “militant” deaths, without further explanation. All reporting of government accounts of “militant” deaths should include acknowledgment that the US government counts all adult males killed by strikes as “militants,” absent exonerating evidence. Media accounts relying on anonymous government sources should also highlight the fact of their single-source information and of the past record of false government reports.
INTRODUCTION

The report is divided into five chapters: Background and Context, Numbers, Living Under Drones, Legal Analysis, and Strategic Considerations. Immediately following is a brief account of the methodology of this study, including challenges faced by our research team. The report then turns to the five main chapters:

'Background and Context,' Chapter 1, provides brief background and context on: the nature of unmanned aerial vehicles; drones and targeted killings as a response to 9/11; Obama’s escalation of the drone program; the decision-making process behind drone strikes; the Pakistani government’s divided role; conflict, non-state groups, and military forces in northwest Pakistan; the Federally Administered Tribal Areas (FATA); and the limits on access to FATA.

'Numbers,' Chapter 2, assesses the debate on drone casualties, outlining the factors that produce conflicting and often unreliable reporting by government and media sources. Examining the methods and content of three well-known and widely cited drone data aggregators, this chapter explains what information can be gleaned from these sources, and challenges the oversimplified civilian/"militant" binary reproduced in many accounts.

'Living under Drones,' Chapter 3 sets forth the core findings of this report. The Chapter begins with firsthand narrative accounts of three specific drone strikes. For each of these strikes, there is significant evidence of civilian casualties. It further examines the broader impacts of drone surveillance and strikes in North Waziristan, including on the families of those killed, education and economic opportunities, emotional trauma, widespread fear, and the undermining of community institutions.

'Legal Analysis,' Chapter 4 provides an overview of the terms of debate on the legality of the US targeted killing program and drone campaign in Pakistan under both international and US domestic law. It describes the law related to key issues: whether US drone practices violate Pakistan’s sovereignty; when and which individuals may lawfully be targeted; and the extent to which the US has met, or failed to meet, its international legal obligations related to transparency and accountability.

'Strategic Considerations,' Chapter 5 examines the strategic implications of US drone strike policies in Pakistan. In particular, it considers available evidence about their effectiveness in hampering attacks by armed non-state actors, their impact on attitudes in Pakistan and the surrounding region toward the US, their geopolitical implications, and their effect on decision-making related to war and the use of force in the US.
The report includes several appendices. The first appendix provides additional narratives from victims and witnesses to drone strikes, as well as others directly affected by drones. The second appendix charts the timing and intensity of drone attacks between January 2010 and June 2012 in light of parallel political events and key moments in Pakistani-US relations. The third appendix compares statements of US officials on drone strikes with strike data reported by a leading strike data aggregator.

**Methodology**

This report is based on over 130 detailed interviews with victims and witnesses of drone activity, their family members, current and former Pakistani government officials, representatives from five major Pakistani political parties, subject matter experts, lawyers, medical professionals, development and humanitarian workers, members of civil society, academics, and journalists. Our research team also engaged in extensive review of documentary sources, including: news reports; legal, historical, political, medical, and other relevant scholarship; civil society and analysts’ reports; court filings and other legal documents; government documents; and physical evidence.

Our research team conducted two separate investigations in Pakistan (including in Islamabad, Peshawar, Lahore, and Rawalpindi) in February-March 2012 and May 2012.\(^{10}\) Investigations included interviews with 69 individuals ("experiential victims") who were witnesses to drone strikes or surveillance, victims of strikes, or family members of victims from North Waziristan.\(^{11}\) These interviewees provided first-hand accounts of drone strikes, and provided testimony about a range of issues, including the missile strikes themselves, the strike sites, the victims' bodies, or a family member or members killed or injured in the strike.\(^{12}\) They also provided testimony about the impacts of drone surveillance and attacks on their daily lives, and their views of US policy.

---

\(^{10}\) Our researchers did not conduct *in situ* investigations in the drone-affected areas of FATA because of security risks at the time of our investigations, and because the Pakistani military prevents foreigners and non-FATA residents from accessing the region.

\(^{11}\) A majority of the interviewees brought school- or government-issued photo identification cards to the interview indicating their residence in North Waziristan.

\(^{12}\) We have defined "close family member" as a member of the interviewee's household. In Waziri culture, households can include grandparents, parents, siblings, and children, as well as uncles, aunts, or cousins.
Interviews were arranged through local contacts in Pakistan, including journalists, lawyers, tribal leaders, experts, and civil society members. The majority of the experiential victims interviewed were arranged with the assistance of the Foundation for Fundamental Rights, a legal nonprofit based in Islamabad that has become the most prominent legal advocate for drone victims in Pakistan. Those interviewees, who undertook an extremely unsafe, time-consuming, and difficult trip in order to be interviewed, were all male, as poor security conditions, together with cultural norms of purda (separation of men and women), restricted women's ability to travel. One of the experiential victims interviewed is a female Waziri now residing outside Federally Administered Tribal Areas (FATA). Nine of the 69 experiential victims are clients of the Foundation for Fundamental Rights. None of the interviewees were provided compensation for participating in investigations for this report.13

The interviews were conducted by teams that included at least one Stanford or NYU researcher, as well as a translator. Some interviews also included a researcher from either Reprieve or the Foundation for Fundamental Rights. The interviews with individual Waziris were semi-structured, and lasted from approximately thirty minutes to two hours.

Security, confidentiality, and privacy for those interviewed were key concerns. Our research team applied informed consent guidelines to all interviews, and interviewees chose if or how they wished to be identified in this report. We do not include the names and other identifying information of interviewed individuals in this report when so requested by the person concerned, or when the research team determined that doing so might place the individual at risk. Thus, many of the experiential victims have been given pseudonyms in this report. All of the medical and humanitarian professionals, and most of the journalists with whom we met, also expressed concerns for their safety, and requested anonymity.

In addition to our interviews with medical professionals in Pakistan, medical experts at Stanford reviewed this report's sections concerning the psychological and physiological impacts of drones. These experts also met with our research team to discuss our findings and assist in our analysis of the classification of symptoms.

13 The Foundation for Fundamental Rights and Reprieve organized and financed the transportation to Islamabad and Peshawar for the majority of experiential victims. The Stanford Clinic paid for the translation services and rental of the space used for interviewing in both Peshawar and Islamabad.
As part of our effort to speak with relevant stakeholders, our research team requested
the input of the US government, and sought to share our findings in advance of this
report's release. Via letter sent July 18, 2012, we requested a meeting with the National
Security Council (NSC), “the President's principal arm for coordinating [national
security and foreign] policies among various government agencies.”14 At this writing, we
had not received a response to our request.

CHALLENGES

The foremost challenge the research team faced was the pervasive lack of US
government transparency about its targeted killing and drone policies and practices in
Pakistan. This secrecy forced us to conduct challenging primary research into the effects
of drones in Pakistan. Primary research in FATA is difficult for many reasons.

First, it is very difficult for foreigners physically to access FATA, partly due to the
Pakistani government’s efforts to block access through heavily guarded checkpoints, and
partly due to serious security risks.

Second, it is very difficult for residents of Waziristan to travel out of the region. Those
we interviewed had to travel hundreds of kilometers by road to reach Islamabad or
Peshawar, in journeys that could take anywhere from eight hours to several days, and
which required passing through dozens of military and police checkpoint stops, as well
as, in some cases, traveling through active fighting between armed non-state groups and
Pakistani forces.

Third, mistrust, often justifiable, from many in FATA toward outsiders (particularly
Westerners) inhibits ready access to individuals and communities.

Fourth, many residents of FATA fear retribution from all sides—Pakistani military,
intelligence services, non-state armed groups—for speaking with outsiders about the
issues raised in this report.

14 WHITE HOUSE, NATIONAL SECURITY COUNCIL, http://www.whitehouse.gov/administration/eop/nse (last
visited Sept. 12, 2012). We requested a meeting with US Deputy National Security Advisor Denis
McDonough.
Fifth, practices of purda in FATA make it extremely difficult for women to travel, for outsiders to speak directly to Waziri females, or to obtain information about females through male family members. It is often considered inappropriate, for example, for men to provide the names of female victims of drone strikes. In addition, strict segregation can mean that neighbors or extended family members may not know how many women and children were killed or injured in a strike. Because of these obstacles to speaking directly with women, most of the information the research team obtained about the impacts of drones on the daily lives of women came second-hand through husbands, sons, fathers, and in-laws, as well as by health care providers and members of civil society working in the area. Following interactions and the building of trust between our researchers and interviewees, a number of those interviewed expressed an interest in facilitating interviews with female witnesses and victims in future investigations.

Sixth, and as documented in the ‘Background and Context’ Chapter, FATA has very low literacy rates. This, in conjunction with the fact that much information about incidents in Waziristan is not recorded in written form, made it difficult for some interviewees to pinpoint the exact dates of certain strikes or to identify in terms that could be related to outsiders the precise geographical locations of small villages. The research team has made extensive efforts to check information provided by interviewees against that provided in other interviews, known general background information, other reports and investigations, media reports, and physical evidence wherever possible. Many of the interviewees provided victims’ identification cards and some shared photographs of victims and strike sites, or medical records documenting their injuries. We also reviewed pieces of missile shrapnel.

Full article can be downloaded at:

http://livingunderdrones.org

15 Extended family households can be quite large; one interviewee, for instance, told us he lives in a large extended family compound of 50-60 relatives. Interview with Ibrahim Shah, in Islamabad, Pakistan (May 9, 2012).
SUPREME COURT OF THE UNITED STATES

SYLLABUS

UNITED STATES v. JONES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT


The Government obtained a search warrant permitting it to install a Global-Positioning-System (GPS) tracking device on a vehicle registered to respondent Jones's wife. The warrant authorized installation in the District of Columbia and within 10 days, but agents installed the device on the 11th day and in Maryland. The Government then tracked the vehicle's movements for 28 days. It subsequently secured an indictment of Jones and others on drug trafficking conspiracy charges. The District Court suppressed the GPS data obtained while the vehicle was parked at Jones's residence, but held the remaining data admissible because Jones had no reasonable expectation of privacy when the vehicle was on public streets. Jones was convicted. The D. C. Circuit reversed, concluding that admission of the evidence obtained by warrantless use of the GPS device violated the Fourth Amendment.

Held: The Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment. Pp. 3–12.

(a) The Fourth Amendment protects the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” Here, the Government's physical intrusion on an “effect” for the purpose of obtaining information constitutes a “search.” This type of encroachment on an area enumerated in the Amendment would have been considered a search within the meaning of the Amendment at the time it was adopted. Pp. 3–4.

(b) This conclusion is consistent with this Court's Fourth Amendment jurisprudence, which until the latter half of the 20th century was tied to common-law trespass. Later cases, which have deviated from that exclusively property-based approach, have applied the
Syllabus

analysis of Justice Harlan’s concurrence in *Katz v. United States*, 389 U. S. 347, which said that the Fourth Amendment protects a person’s “reasonable expectation of privacy,” *id.*, at 360. Here, the Court need not address the Government’s contention that Jones had no “reasonable expectation of privacy,” because Jones’s Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, the Court must “assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Kyllo v. United States*, 533 U. S. 27, 34. *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. The *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test. *See Alderman v. United States*, 394 U. S. 165, 176; *Soldal v. Cook County*, 506 U. S. 56, 64. *United States v. Knotts*, 460 U. S. 276, and *United States v. Karo*, 468 U. S. 705—post-*Katz* cases rejecting Fourth Amendment challenges to “beepers,” electronic tracking devices representing another form of electronic monitoring—do not foreclose the conclusion that a search occurred here. *New York v. Class*, 475 U. S. 106, and *Oliver v. United States*, 466 U. S. 170, also do not support the Government’s position. Pp. 4–12.

(c) The Government’s alternative argument—that if the attachment and use of the device was a search, it was a reasonable one—is forfeited because it was not raised below. P. 12.

615 F. 3d 544, affirmed.

SCALIA, J., delivered the opinion of the Court, in which ROBERTS, C. J., and KENNEDY, THOMAS, and SOTOMAYOR, JJ., joined. SOTOMAYOR, J., filed a concurring opinion. ALITO, J., filed an opinion concurring in the judgment, in which GINSBURG, BREYER, and KAGAN, JJ., joined.
Opinion of the Court

NOTICE: This opinion is subject to formal revision before publication in the preliminary print of the United States Reports. Readers are requested to notify the Reporter of Decisions, Supreme Court of the United States, Washington, D.C. 20543, of any typographical or other formal errors, in order that corrections may be made before the preliminary print goes to press.

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER v. ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE SCALIA delivered the opinion of the Court.

We decide whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment.

I

In 2004 respondent Antoine Jones, owner and operator of a nightclub in the District of Columbia, came under suspicion of trafficking in narcotics and was made the target of an investigation by a joint FBI and Metropolitan Police Department task force. Officers employed various investigative techniques, including visual surveillance of the nightclub, installation of a camera focused on the front door of the club, and a pen register and wiretap covering Jones's cellular phone.

Based in part on information gathered from these sources, in 2005 the Government applied to the United States District Court for the District of Columbia for a warrant authorizing the use of an electronic tracking device on the Jeep Grand Cherokee registered to Jones's
wife. A warrant issued, authorizing installation of the device in the District of Columbia and within 10 days.

On the 11th day, and not in the District of Columbia but in Maryland, agents installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot. Over the next 28 days, the Government used the device to track the vehicle’s movements, and once had to replace the device’s battery when the vehicle was parked in a different public lot in Maryland. By means of signals from multiple satellites, the device established the vehicle’s location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period.

The Government ultimately obtained a multiple-count indictment charging Jones and several alleged co-conspirators with, as relevant here, conspiracy to distribute and possess with intent to distribute five kilograms or more of cocaine and 50 grams or more of cocaine base, in violation of 21 U. S. C. §§841 and 846. Before trial, Jones filed a motion to suppress evidence obtained through the GPS device. The District Court granted the motion only in part, suppressing the data obtained while the vehicle was parked in the garage adjoining Jones’s residence. 451 F. Supp. 2d 71, 88 (2006). It held the remaining data admissible, because “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” Ibid. (quoting United States v. Knotts, 460 U. S. 276, 281 (1983)). Jones’s trial in October 2006 produced a hung jury on the conspiracy count.

In March 2007, a grand jury returned another indict-

---

1In this litigation, the Government has conceded noncompliance with the warrant and has argued only that a warrant was not required. United States v. Maynard, 615 F. 3d 544, 566, n. (CADC 2010).
ment, charging Jones and others with the same conspiracy. The Government introduced at trial the same GPS-derived locational data admitted in the first trial, which connected Jones to the alleged conspirators’ stash house that contained $850,000 in cash, 97 kilograms of cocaine, and 1 kilogram of cocaine base. The jury returned a guilty verdict, and the District Court sentenced Jones to life imprisonment.


II

A

The Fourth Amendment provides in relevant part that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” It is beyond dispute that a vehicle is an “effect” as that term is used in the Amendment. *United States v. Chadwick*, 433 U. S. 1, 12 (1977). We hold that the Government’s installation of a GPS device on a target’s vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a “search.”

---

2 As we have noted, the Jeep was registered to Jones’s wife. The Government acknowledged, however, that Jones was “the exclusive driver.” Id., at 555, n. (internal quotation marks omitted). If Jones was not the owner he had at least the property rights of a bailee. The Court of Appeals concluded that the vehicle’s registration did not affect his ability to make a Fourth Amendment objection, *ibid.*, and the Government has not challenged that determination here. We therefore do not consider the Fourth Amendment significance of Jones’s status.
Opinion of the Court

It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted. *Entick v. Carrington*, 95 Eng. Rep. 807 (C. P. 1765), is a "case we have described as a 'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the Constitution was adopted, and considered to be 'the true and ultimate expression of constitutional law' with regard to search and seizure. *Brower v. County of Inyo*, 489 U. S. 593, 596 (1989) (quoting *Boyd v. United States*, 116 U. S. 616, 626 (1886)). In that case, Lord Camden expressed in plain terms the significance of property rights in search-and-seizure analysis:

"[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law." *Entick*, supra, at 817.

The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to "the right of the people to be secure against unreasonable searches and seizures"; the phrase "in their persons, houses, papers, and effects" would have been superfluous.

Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century. *Kyllo v. United States*, 533 U. S. 27, 31 (2001); Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 816 (2004). Thus, in *Olmstead v. United States*, 277 U. S.
438 (1928), we held that wiretaps attached to telephone wires on the public streets did not constitute a Fourth Amendment search because "[t]here was no entry of the houses or offices of the defendants," id., at 464.

Our later cases, of course, have deviated from that exclusively property-based approach. In *Katz v. United States*, 389 U. S. 347, 351 (1967), we said that "the Fourth Amendment protects people, not places," and found a violation in attachment of an eavesdropping device to a public telephone booth. Our later cases have applied the analysis of Justice Harlan's concurrence in that case, which said that a violation occurs when government officers violate a person's "reasonable expectation of privacy," id., at 360. See, e.g., *Bond v. United States*, 529 U. S. 334 (2000); *California v. Ciraolo*, 476 U. S. 207 (1986); *Smith v. Maryland*, 442 U. S. 735 (1979).

The Government contends that the Harlan standard shows that no search occurred here, since Jones had no "reasonable expectation of privacy" in the area of the Jeep accessed by Government agents (its underbody) and in the locations of the Jeep on the public roads, which were visible to all. But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, supra, at 34. As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates. *Katz* did not repudiate

---

3 Justice Alito's concurrence (hereinafter concurrence) doubts the wisdom of our approach because "it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case." *Post*, at 3 (opinion concurring in judgment). But in fact it posits a situation that is not far afield—a constable's concealing himself
that understanding. Less than two years later the Court upheld defendants' contention that the Government could not introduce against them conversations between other people obtained by warrantless placement of electronic surveillance devices in their homes. The opinion rejected the dissent's contention that there was no Fourth Amendment violation "unless the conversational privacy of the homeowner himself is invaded."4 Alderman v. United States, 394 U. S. 165, 176 (1969). "[W]e [do not] believe that Katz, by holding that the Fourth Amendment protects persons and their private conversations, was intended to withdraw any of the protection which the Amendment extends to the home..." Id., at 180.

More recently, in Soldal v. Cook County, 506 U. S. 56 (1992), the Court unanimously rejected the argument that although a "seizure" had occurred "in a 'technical' sense" when a trailer home was forcibly removed, id., at 62, no Fourth Amendment violation occurred because law enforcement had not "invade[d] the [individuals'] privacy," id., at 60. Katz, the Court explained, established that "property rights are not the sole measure of Fourth

in the target's coach in order to track its movements. Ibid. There is no doubt that the information gained by that trespassory activity would be the product of an unlawful search—whether that information consisted of the conversations occurring in the coach, or of the destinations to which the coach traveled.

In any case, it is quite irrelevant whether there was an 18th-century analog. Whatever new methods of investigation may be devised, our task, at a minimum, is to decide whether the action in question would have constituted a "search" within the original meaning of the Fourth Amendment. Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.

4Thus, the concurrence's attempt to recast Alderman as meaning that individuals have a "legitimate expectation of privacy in all conversations that [take] place under their roof," post, at 6–7, is foreclosed by the Court's opinion. The Court took as a given that the homeowner's "conversational privacy" had not been violated.
Amendment violations," but did not "snuff[f] out the previously recognized protection for property." 506 U.S., at 64. As Justice Brennan explained in his concurrence in *Knotts, Katz* did not erode the principle "that, when the Government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment." 460 U.S., at 236 (opinion concurring in judgment). We have embodied that preservation of past rights in our very definition of "reasonable expectation of privacy" which we have said to be an expectation "that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (internal quotation marks omitted). *Katz* did not narrow the Fourth Amendment's scope.5

The Government contends that several of our post-*Katz* cases foreclose the conclusion that what occurred here constituted a search. It relies principally on two cases in

---

5The concurrence notes that post-*Katz* we have explained that "an actual trespass is neither necessary nor sufficient to establish a constitutional violation." *Post*, at 6 (quoting *United States v. Karo*, 468 U.S. 705, 713 (1984)). That is undoubtedly true, and undoubtedly irrelevant. *Karo* was considering whether a seizure occurred, and as the concurrence explains, a seizure of property occurs, not when there is a trespass, but "when there is some meaningful interference with an individual's possessory interests in that property." *Post*, at 2 (internal quotation marks omitted). Likewise with a search. Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information.

Related to this, and similarly irrelevant, is the concurrence's point that, if analyzed separately, neither the installation of the device nor its use would constitute a Fourth Amendment search. See *ibid*. Of course not. A trespass on "houses" or "effects," or a *Katz* invasion of privacy, is not alone a search unless it is done to obtain information; and the obtaining of information is not alone a search unless it is achieved by such a trespass or invasion of privacy.
which we rejected Fourth Amendment challenges to “beepers,” electronic tracking devices that represent another form of electronic monitoring. The first case, *Knotts*, upheld against Fourth Amendment challenge the use of a “beeper” that had been placed in a container of chloroform, allowing law enforcement to monitor the location of the container. 460 U. S., at 278. We said that there had been no infringement of Knotts’ reasonable expectation of privacy since the information obtained—the location of the automobile carrying the container on public roads, and the location of the off-loaded container in open fields near Knotts’ cabin—had been voluntarily conveyed to the public.\(^6\) *Id.*, at 281–282. But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test. The holding in *Knotts* addressed only the former, since the latter was not at issue. The beeper had been placed in the container before it came into Knotts’ possession, with the consent of the then-owner. 460 U. S., at 278. Knotts did not challenge that installation, and we specifically declined to consider its effect on the Fourth Amendment analysis. *Id.*, at 279, n. *Knotts* would be relevant, perhaps, if the Government were making the argument that what would otherwise be an unconstitutional search is not such where it produces only public information. The Government does not make that argument, and we know of no case that would support it.

The second “beeper” case, *United States v. Karo*, 468 U. S. 705 (1984), does not suggest a different conclusion. There we addressed the question left open by *Knotts*, whether the installation of a beeper in a container

---

\(^6\) *Knotts* noted the “limited use which the government made of the signals from this particular beeper,” 460 U. S., at 284; and reserved the question whether “different constitutional principles may be applicable” to “dragnet-type law enforcement practices” of the type that GPS tracking made possible here, *ibid.*
amounted to a search or seizure. 468 U. S., at 713. As in
Knotts, at the time the beeper was installed the container
belonged to a third party, and it did not come into posses-
sion of the defendant until later. 468 U. S., at 708. Thus,
the specific question we considered was whether the in-
stallation "with the consent of the original owner consti-
tute[d] a search or seizure . . . when the container is deliv-
ered to a buyer having no knowledge of the presence of the
beeper." Id., at 707 (emphasis added). We held not. The
Government, we said, came into physical contact with
the container only before it belonged to the defendant Karo;
and the transfer of the container with the unmonitored
beeper inside did not convey any information and thus did
not invade Karo's privacy. See id., at 712. That conclu-
sion is perfectly consistent with the one we reach here.
Karo accepted the container as it came to him, beeper and
all, and was therefore not entitled to object to the beeper's
presence, even though it was used to monitor the contain-
er's location. Cf. On Lee v. United States, 343 U. S. 747,
751-752 (1952) (no search or seizure where an informant,
who was wearing a concealed microphone, was invited into
the defendant's business). Jones, who possessed the Jeep
at the time the Government trespassorilly inserted the
information-gathering device, is on much different footing.
The Government also points to our exposition in New
York v. Class, 475 U. S. 106 (1986), that "[t]he exterior of
a car . . . is thrust into the public eye, and thus to examine
it does not constitute a 'search.'" Id., at 114. That state-
ment is of marginal relevance here since, as the Govern-
ment acknowledges, "the officers in this case did more
than conduct a visual inspection of respondent's vehicle,"
Brief for United States 41 (emphasis added). By attaching
the device to the Jeep, officers encroached on a protected
area. In Class itself we suggested that this would make a
difference, for we concluded that an officer's momentary
reaching into the interior of a vehicle did constitute a
search.\textsuperscript{7} 475 U. S., at 114–115.

Finally, the Government's position gains little support from our conclusion in \textit{Oliver v. United States}, 466 U. S. 170 (1984), that officers' information-gathering intrusion on an "open field" did not constitute a Fourth Amendment search even though it was a trespass at common law, \textit{id.}, at 183. Quite simply, an open field, unlike the curtilage of a home, see \textit{United States v. Dunn}, 480 U. S. 294, 300 (1987), is not one of those protected areas enumerated in the Fourth Amendment. \textit{Oliver, supra}, at 176–177. See also \textit{Hester v. United States}, 265 U. S. 57, 59 (1924). The Government's physical intrusion on such an area—unlike its intrusion on the "effect" at issue here—is of no Fourth Amendment significance.\textsuperscript{8}

\textbf{B}

The concurrence begins by accusing us of applying "18th-century tort law." \textit{Post}, at 1. That is a distortion. What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide at

\textsuperscript{7}The Government also points to \textit{Cardwell v. Lewis}, 417 U. S. 583 (1974), in which the Court rejected the claim that the inspection of an impounded vehicle's tire tread and the collection of paint scrapings from its exterior violated the Fourth Amendment. Whether the plurality said so because no search occurred or because the search was reasonable is unclear. Compare \textit{id.}, at 591 (opinion of Blackmun, J.) ("[W]e fail to comprehend what expectation of privacy was infringed"), with \textit{id.}, at 592 ("Under circumstances such as these, where probable cause exists, a warrantless examination of the exterior of a car is not unreasonable ... ").

\textsuperscript{8}Thus, our theory is not that the Fourth Amendment is concerned with "any technical trespass that led to the gathering of evidence." \textit{Post}, at 3 (ALITO, J., concurring in judgment) (emphasis added). The Fourth Amendment protects against trespassory searches only with regard to those items ("persons, houses, papers, and effects") that it enumerates. The trespass that occurred in \textit{Oliver} may properly be understood as a "search," but not one "in the constitutional sense." 466 U. S., at 170, 183.
a minimum the degree of protection it afforded when it was adopted. The concurrence does not share that belief. It would apply exclusively Katz’s reasonable-expectation-of-privacy test, even when that eliminates rights that previously existed.

The concurrence faults our approach for “present[ing] particularly vexing problems” in cases that do not involve physical contact, such as those that involve the transmission of electronic signals. Post, at 9. We entirely fail to understand that point. For unlike the concurrence, which would make Katz the exclusive test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis.

In fact, it is the concurrence’s insistence on the exclusivity of the Katz test that needlessly leads us into “particularly vexing problems” in the present case. This Court has to date not deviated from the understanding that mere visual observation does not constitute a search. See Kyllo, 533 U. S., at 31–32. We accordingly held in Knotts that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” 460 U. S., at 281. Thus, even assuming that the concurrence is correct to say that “[t]raditional surveillance” of Jones for a 4-week period “would have required a large team of agents, multiple vehicles, and perhaps aerial assistance,” post, at 12, our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.

And answering it affirmatively leads us needlessly into additional thorny problems. The concurrence posits that “relatively short-term monitoring of a person’s movement’s
Opinion of the Court

on public streets" is okay, but that "the use of longer term GPS monitoring in investigations of most offenses" is no good. Post, at 13 (emphasis added). That introduces yet another novelty into our jurisprudence. There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offense[s]" which may permit longer observation. See post, at 13–14. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist? We may have to grapple with these "vexing problems" in some future case where a classic trespassory search is not involved and resort must be had to Katz analysis; but there is no reason for rushing forward to resolve them here.

III

The Government argues in the alternative that even if the attachment and use of the device was a search, it was reasonable—and thus lawful—under the Fourth Amendment because "officers had reasonable suspicion, and indeed probable cause, to believe that [Jones] was a leader in a large-scale cocaine distribution conspiracy." Brief for United States 50–51. We have no occasion to consider this argument. The Government did not raise it below, and the D. C. Circuit therefore did not address it. See 625 F. 3d, at 767 (Ginsburg, Tatel, and Griffith, JJ., concurring in denial of rehearing en banc). We consider the argument forfeited. See Sprietsma v. Mercury Marine, 537 U. S. 51, 56, n. 4 (2002).

* * *

The judgment of the Court of Appeals for the D. C. Circuit is affirmed.

It is so ordered.
Cite as: 565 U. S. ____ (2012)

SOTOMAYOR, J., concurring

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER v. ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE SOTOMAYOR, concurring.

I join the Court’s opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, “[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area.” Ante, at 6, n. 3. In this case, the Government installed a Global Positioning System (GPS) tracking device on respondent Antoine Jones’ Jeep without a valid warrant and without Jones’ consent, then used that device to monitor the Jeep’s movements over the course of four weeks. The Government usurped Jones’ property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection. See, e.g., Silverman v. United States, 365 U. S. 505, 511–512 (1961).

Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property. See, e.g., Kyllo v. United States, 533 U. S. 27, 31–33 (2001). Rather, even in the absence of a trespass, “a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.” Id., at 33; see also Smith v. Maryland, 442 U. S. 735, 740–741 (1979); Katz v. United States, 389 U. S. 347, 361 (1967) (Harlan, J., concurring). In Katz, this Court enlarged its then-prevailing focus on property rights by announcing
that the reach of the Fourth Amendment does not "turn upon the presence or absence of a physical intrusion." *Id.*, at 353. As the majority's opinion makes clear, however, *Katz's* reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it. *Ante*, at 8. Thus, "when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment." *United States v. Knotts*, 460 U. S. 276, 286 (1983) (Brennan, J., concurring in judgment); see also, *Rakas v. Illinois*, 439 U. S. 128, 144, n. 12 (1978). JUSTICE ALITO's approach, which discounts altogether the constitutional relevance of the Government's physical intrusion on Jones' Jeep, erodes that longstanding protection for privacy expectations inherent in items of property that people possess or control. See *post*, at 5–7 (opinion concurring in judgment). By contrast, the trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.

Nonetheless, as JUSTICE ALITO notes, physical intrusion is now unnecessary to many forms of surveillance. *Post*, at 9–12. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. See *United States v. Pineda-Moreno*, 617 F. 3d 1120, 1125 (CA9 2010) (Kozinski, C. J., dissenting from denial of rehearing en banc). In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But "[s]ituations involving merely the transmission of electronic signals without trespass
would remain subject to Katz analysis." Ante, at 11. As JUSTICE ALITO incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the Katz test by shaping the evolution of societal privacy expectations. Post, at 10–11. Under that rubric, I agree with JUSTICE ALITO that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Post, at 13.

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, e.g., People v. Weaver, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. Pineda-Moreno, 617 F. 3d, at 1124 (opinion of Kozinski, C. J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." Illinois v. Lidster, 540 U. S. 419, 426 (2004).

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net
result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." United States v. Cuevas-Perez, 640 F. 3d 272, 285 (CA7 2011) (Plaum, J., concurring).

I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques. See Kyllo, 533 U. S., at 35, n. 2; ante, at 11 (leaving open the possibility that duplicating traditional surveillance "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy"). I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance," United States v. Di Re, 332 U. S. 581, 595 (1948).*

*United States v. Knotts, 460 U. S. 276 (1983), does not foreclose the conclusion that GPS monitoring, in the absence of a physical intrusion, is a Fourth Amendment search. As the majority's opinion notes, Knotts reserved the question whether "different constitutional principles may be applicable" to invasive law enforcement practices such as GPS tracking. See ante, at 8, n. 6 (quoting 460 U. S., at 284).

United States v. Karo, 468 U. S. 705 (1984), addressed the Fourth
SOTOMAYOR, J., concurring

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g.*, *Smith*, 442 U. S., at 742; *United States v. Miller*, 425 U. S. 435, 443 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as JUSTICE ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post*, at 10, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases

Amendment implications of the installation of a beeper in a container with the consent of the container's original owner, who was aware that the beeper would be used for surveillance purposes. *Id.*, at 707. Owners of GPS-equipped cars and smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements. To the contrary, subscribers of one such service greeted a similar suggestion with anger. Quain, Changes to OnStar's Privacy Terms Rile Some Users, N. Y. Times (Sept. 22, 2011), online at http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users (as visited Jan. 19, 2012, and available in Clerk of Court's case file). In addition, the bugged container in *Karo* lacked the close relationship with the target that a car shares with its owner. The bugged container in *Karo* was stationary for much of the Government's surveillance. See 468 U. S., at 708–710. A car's movements, by contrast, are its owner's movements.
to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith*, 442 U.S., at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U.S., at 351–352 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision. I therefore join the majority's opinion.
ALITO, J., concurring in judgment

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER v. ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE ALITO, with whom JUSTICE GINSBURG, JUSTICE BREYER, and JUSTICE KAGAN join, concurring in the judgment.

This case requires us to apply the Fourth Amendment’s prohibition of unreasonable searches and seizures to a 21st-century surveillance technique, the use of a Global Positioning System (GPS) device to monitor a vehicle’s movements for an extended period of time. Ironically, the Court has chosen to decide this case based on 18th-century tort law. By attaching a small GPS device to the underside of the vehicle that respondent drove, the law enforcement officers in this case engaged in conduct that might have provided grounds in 1791 for a suit for trespass to chattels. And for this reason, the Court concludes, the installation and use of the GPS device constituted a search. Ante, at 3–4.

1 Although the record does not reveal the size or weight of the device used in this case, there is now a device in use that weighs two ounces and is the size of a credit card. Tr. of Oral Arg. 27.

2 At common law, a suit for trespass to chattels could be maintained if there was a violation of “the dignitary interest in the inviolability of chattels,” but today there must be “some actual damage to the chattel before the action can be maintained.” W. Keeton, D. Dobbs, R. Keeton, & D. Owen, Prosser & Keeton on Law of Torts 87 (5th ed. 1984) (hereinafter Prosser & Keeton). Here, there was no actual damage to the vehicle to which the GPS device was attached.
This holding, in my judgment, is unwise. It strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial.

I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.

I

A

The Fourth Amendment prohibits "unreasonable searches and seizures," and the Court makes very little effort to explain how the attachment or use of the GPS device fits within these terms. The Court does not contend that there was a seizure. A seizure of property occurs when there is "some meaningful interference with an individual's possessory interests in that property," United States v. Jacobsen, 466 U. S. 109, 113 (1984), and here there was none. Indeed, the success of the surveillance technique that the officers employed was dependent on the fact that the GPS did not interfere in any way with the operation of the vehicle, for if any such interference had been detected, the device might have been discovered.

The Court does claim that the installation and use of the GPS constituted a search, see ante, at 3–4, but this conclusion is dependent on the questionable proposition that these two procedures cannot be separated for purposes of Fourth Amendment analysis. If these two procedures are analyzed separately, it is not at all clear from the Court's opinion why either should be regarded as a search. It is clear that the attachment of the GPS device was not itself a search; if the device had not functioned or if the officers had not used it, no information would have been obtained. And the Court does not contend that the use of the device constituted a search either. On the contrary, the Court
ALITO, J., concurring in judgment

accepts the holding in United States v. Knotts, 460 U. S. 276 (1983), that the use of a surreptitiously planted electronic device to monitor a vehicle's movements on public roads did not amount to a search. See ante, at 7.

The Court argues—and I agree—that “we must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” Ante, at 5 (quoting Kyilo v. United States, 533 U. S. 27, 34 (2001)). But it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?) The Court's theory seems to be that the concept of a search, as originally understood, comprehended any technical trespass that led to the gathering of evidence, but we know that this is incorrect. At common law, any unauthorized intrusion on private property was actionable, see Prosser & Keeton 75, but a trespass on open fields, as opposed to the “curtilage” of a home, does not fall within the scope of the Fourth Amendment because private property outside the curtilage is not part of a “house[e]” within the meaning of the Fourth Amendment. See Oliver v. United States, 466 U. S. 170 (1984); Hester v. United States, 265 U. S. 57 (1924).

B

The Court's reasoning in this case is very similar to that in the Court's early decisions involving wiretapping and electronic eavesdropping, namely, that a technical trespass followed by the gathering of evidence constitutes a

---

3 The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.
search. In the early electronic surveillance cases, the Court concluded that a Fourth Amendment search occurred when private conversations were monitored as a result of an "unauthorized physical penetration into the premises occupied" by the defendant. *Silverman v. United States*, 365 U.S. 505, 509 (1961). In *Silverman*, police officers listened to conversations in an attached home by inserting a "spike mike" through the wall that this house shared with the vacant house next door. *Id.*, at 506. This procedure was held to be a search because the mike made contact with a heating duct on the other side of the wall and thus "usurp[ed] . . . an integral part of the premises." *Id.*, at 511.

By contrast, in cases in which there was no trespass, it was held that there was no search. Thus, in *Olmstead v. United States*, 277 U. S. 438 (1928), the Court found that the Fourth Amendment did not apply because "[t]he taps from house lines were made in the streets near the houses." *Id.*, at 457. Similarly, the Court concluded that no search occurred in *Goldman v. United States*, 316 U. S. 129, 135 (1942), where a "detectaphone" was placed on the outer wall of defendant's office for the purpose of overhearing conversations held within the room.

This trespass-based rule was repeatedly criticized. In *Olmstead*, Justice Brandeis wrote that it was "immaterial where the physical connection with the telephone wires was made." 277 U. S., at 479 (dissenting opinion). Although a private conversation transmitted by wire did not fall within the literal words of the Fourth Amendment, he argued, the Amendment should be understood as prohibiting "every unjustifiable intrusion by the government upon the privacy of the individual." *Id.*, at 478. See also, e.g., *Silverman*, supra, at 513 (Douglas, J., concurring) ("The concept of 'an unauthorized physical penetration into the premises,' on which the present decision rests seems to me beside the point. Was not the wrong . . . done when the
ALITO, J., concurring in judgment

intimacies of the home were tapped, recorded, or revealed? The depth of the penetration of the electronic device—even the degree of its remoteness from the inside of the house—is not the measure of the injury’); Goldman, supra, at 139 (Murphy, J., dissenting) (’’[T]he search of one’s home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person’s privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment’’).

Katz v. United States, 389 U. S. 347 (1967), finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation. Katz involved the use of a listening device that was attached to the outside of a public telephone booth and that allowed police officers to eavesdrop on one end of the target’s phone conversation. This procedure did not physically intrude on the area occupied by the target, but the Katz Court, “repudiate[ed]” the old doctrine, Rakas v. Illinois, 439 U. S. 128, 143 (1978), and held that “[t]he fact that the electronic device employed . . . did not happen to penetrate the wall of the booth can have no constitutional significance,” 389 U. S., at 353 (“[T]he reach of th[e] [Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure”); see Rakas, supra, at 143 (describing Katz as holding that the “capacity to claim the protection for the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place”); Kyllo, supra, at 32 (“We have since decoupled violation of a person’s Fourth Amendment rights from trespassory violation of his property”). What mattered, the Court now held, was whether the conduct at issue “violated the privacy upon which [the defendant] justifiably relied while using the telephone booth.” Katz, supra,
ALITO, J., concurring in judgment

at 353.

Under this approach, as the Court later put it when addressing the relevance of a technical trespass, "an actual trespass is neither necessary nor sufficient to establish a constitutional violation." United States v. Karo, 468 U.S. 705, 713 (1984) (emphasis added). Ibid. ("Compar[ing] Katz v. United States, 389 U.S. 347 (1967) (no trespass, but Fourth Amendment violation), with Oliver v. United States, 466 U.S. 170 (1984) (trespass, but no Fourth Amendment violation")). In Oliver, the Court wrote:

"The existence of a property right is but one element in determining whether expectations of privacy are legitimate. The premise that property interests control the right of the Government to search and seize has been discredited." Katz, 389 U.S., at 353, (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967); some internal quotation marks omitted)." 466 U.S., at 183.

II

The majority suggests that two post-Katz decisions—Soldal v. Cook County, 506 U.S. 56 (1992), and Alderman v. United States, 394 U.S. 165 (1969)—show that a technical trespass is sufficient to establish the existence of a search, but they provide little support.

In Soldal, the Court held that towing away a trailer home without the owner’s consent constituted a seizure even if this did not invade the occupants’ personal privacy. But in the present case, the Court does not find that there was a seizure, and it is clear that none occurred.

In Alderman, the Court held that the Fourth Amendment rights of homeowners were implicated by the use of a surreptitiously planted listening device to monitor third-party conversations that occurred within their home. See 394 U.S., at 176–180. Alderman is best understood to
mean that the homeowners had a legitimate expectation of privacy in all conversations that took place under their roof. See *Rakas*, 439 U. S., at 144, n. 12 (citing *Alderman* for the proposition that "the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment"); 439 U. S., at 153 (Powell, J., concurring) (citing *Alderman* for the proposition that "property rights reflect society's explicit recognition of a person's authority to act as he wishes in certain areas, and therefore should be considered in determining whether an individual's expectations of privacy are reasonable"); *Karo, supra*, at 732 (Stevens, J., concurring in part and dissenting in part) (citing *Alderman* in support of the proposition that "a homeowner has a reasonable expectation of privacy in the contents of his home, including items owned by others").

In sum, the majority is hard pressed to find support in post-*Katz* cases for its trespass-based theory.

III

Disharmony with a substantial body of existing case law is only one of the problems with the Court's approach in this case.

I will briefly note four others. First, the Court's reasoning largely disregards what is really important (the use of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation). Attaching such an object is generally regarded as so trivial that it does not provide a basis for recovery under modern tort law. See Prosser & Keeton §14, at 87 (harmless or trivial contact with personal property not actionable); D. Dobbs, Law of Torts 124 (2000) (same). But under the Court's reasoning, this conduct
may violate the Fourth Amendment. By contrast, if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court’s theory would provide no protection.

Second, the Court’s approach leads to incongruous results. If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court’s theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints.

In the present case, the Fourth Amendment applies, the Court concludes, because the officers installed the GPS device after respondent’s wife, to whom the car was registered, turned it over to respondent for his exclusive use. See ante, at 8. But if the GPS had been attached prior to that time, the Court’s theory would lead to a different result. The Court proceeds on the assumption that respondent “had at least the property rights of a bailee,” ante, at 3, n. 2, but a bailee may sue for a trespass to chattel only if the injury occurs during the term of the bailment. See 8A Am. Jur. 2d, Bailment §166, pp. 685–686 (2009). So if the GPS device had been installed before respondent’s wife gave him the keys, respondent would have no claim for trespass—and, presumably, no Fourth Amendment claim either.

Third, under the Court’s theory, the coverage of the Fourth Amendment may vary from State to State. If the events at issue here had occurred in a community property State or a State that has adopted the Uniform Marital

---

Property Act, respondent would likely be an owner of the vehicle, and it would not matter whether the GPS was installed before or after his wife turned over the keys. In non-community-property States, on the other hand, the registration of the vehicle in the name of respondent's wife would generally be regarded as presumptive evidence that she was the sole owner. See 60 C. J. S., Motor Vehicles §231, pp. 398–399 (2002); 8 Am. Jur. 2d, Automobiles §1208, pp. 859–860 (2007).

Fourth, the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked. For example, suppose that the officers in the present case had followed respondent by surreptitiously activating a stolen vehicle detection system that came with the car when it was purchased. Would the sending of a radio signal to activate this system constitute a trespass to chattels? Trespass to chattels has traditionally required a physical touching of the property. See Restatement (Second) of Torts §217 and Comment e (1963 and 1964); Dobbs, supra, at 123. In recent years, courts have wrestled with the application of this old tort in cases involving unwanted electronic contact with computer systems, and some have held that even the transmission of electrons that occurs when a communication is sent from one computer to another is enough. See, e.g., CompuServe, Inc. v. Cyber Promotions, Inc. 962 F. Supp. 1015, 1021 (SD Ohio 1997); Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1566, n. 6 (1996). But may such decisions be followed in applying the Court's trespass theory? Assuming that what matters under the Court's theory is the law of trespass as it existed at the time of the adoption of the Fourth

---

Amendment, do these recent decisions represent a change in the law or simply the application of the old tort to new situations?

IV

A

The *Katz* expectation-of-privacy test avoids the problems and complications noted above, but it is not without its own difficulties. It involves a degree of circularity, see *Kyllo*, 533 U. S., at 34, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. See *Minnesota v. Carter*, 525 U. S. 83, 97 (1998) (SCALIA, J., concurring). In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.\(^6\)

On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress

---

did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U. S. C. §§2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.\(^7\) In an ironic sense, although \textit{Katz} overruled \textit{Olmstead}, Chief Justice Taft's suggestion in the latter case that the regulation of wiretapping was a matter better left for Congress, see 277 U. S., at 465–466, has been borne out.

B

Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.

Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States.\(^8\) For older phones, the accuracy of the location information depends on the density of the tower network, but new "smart phones," which


are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone’s location and speed of movement and can then report back real-time traffic conditions after combining (“crowdsourcing”) the speed of all such phones on any particular road.9 Similarly, phone-location-tracking services are offered as “social” tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person’s expectations about the privacy of his or her daily movements.

V

In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.10 Only an investigation of unusual importance could have justified such an


10Even with a radio transmitter like those used in United States v. Knotts, 460 U.S. 276 (1983), or United States v. Karo, 468 U.S. 705 (1984), such long-term surveillance would have been exceptionally demanding. The beepers used in those cases merely “emit[ted] periodic signals that [could] be picked up by a radio receiver.” Knotts, 460 U.S., at 277. The signal had a limited range and could be lost if the police did not stay close enough. Indeed, in Knotts itself, officers lost the signal from the beeper, and only “with the assistance of a monitoring device located in a helicopter [was] the approximate location of the signal . . . picked up again about one hour later.” Id., at 278.
ALITO, J., concurring in judgment

expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. See, e.g., Kerr, 102 Mich. L. Rev., at 805–806. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.

To date, however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes. The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.

Under this approach, relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See Knotts, 460 U.S., at 281–282. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveil
lance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant.\textsuperscript{11} We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.

* * *

For these reasons, I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment. I therefore agree with the majority that the decision of the Court of Appeals must be affirmed.

\textsuperscript{11}In this case, the agents obtained a warrant, but they did not comply with two of the warrant’s restrictions: They did not install the GPS device within the 10-day period required by the terms of the warrant and by Fed. Rule Crim. Proc. 41(e)(2)(B)(i), and they did not install the GPS device within the District of Columbia, as required by the terms of the warrant and by 18 U.S.C. §3117(a) and Rule 41(b)(4). In the courts below the Government did not argue, and has not argued here, that the Fourth Amendment does not impose these precise restrictions and that the violation of these restrictions does not demand the suppression of evidence obtained using the tracking device. See, e.g., United States v. Gerber, 994 F.2d 1556, 1559–1560 (CA11 1993); United States v. Burke, 517 F.2d 377, 386–387 (CA2 1975). Because it was not raised, that question is not before us.