CONFERENCE MATERIAL

DAY TWO

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

OCTOBER 31—NOVEMBER 1, 2013

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

### Panel IV

**International Organized Crime and National Security**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security</td>
<td>1</td>
</tr>
<tr>
<td>Latin American Criminal Organizations Threaten United States National Security - Luz Nagle</td>
<td>31</td>
</tr>
<tr>
<td>To What Extent Do Global Terrorism and Organized Criminality Converge? - Luis de la Corte Ibanez</td>
<td>37</td>
</tr>
<tr>
<td>Fighting Against Organized Crime and the Action’s Influence on the National Security Enforcement - Alin Pahontu</td>
<td>65</td>
</tr>
<tr>
<td>Terrorism and Transnational Crime: Foreign Policy Issues for Congress - John Rollins &amp; Liana Sun Wyler</td>
<td>73</td>
</tr>
</tbody>
</table>

### Panel V

**Cybersecurity: Future Challenges**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A checklist for what to do “before and after” a data breach - Steven R. Chabinsky</td>
<td>113</td>
</tr>
<tr>
<td>Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line - Steven R. Chabinsky</td>
<td>114</td>
</tr>
<tr>
<td>Cyber-intruder Sparks Massive Federal Response and Debate Over Dealing with Threats - Ellen Nakashima</td>
<td>139</td>
</tr>
<tr>
<td>United States v. Jones - Supreme Court of the United States</td>
<td>147</td>
</tr>
<tr>
<td>Executive Order 13636 - Improving Critical Infrastructure Cybersecurity</td>
<td>169</td>
</tr>
<tr>
<td>Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience</td>
<td>177</td>
</tr>
<tr>
<td>Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch - David J. Barron</td>
<td>189</td>
</tr>
<tr>
<td>The Developing Legal Framework for Defensive and Offensive Cyber Operations - Steven G. Bradbury</td>
<td>195</td>
</tr>
<tr>
<td>The Hackback Debate - Stewart Baker, Orin Kerr and Eugene Volokh</td>
<td>217</td>
</tr>
</tbody>
</table>

### Panel VI

**Ethical Issues Facing Lawyers Practicing National Security Law**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Rules of Professional Conduct: Preamble &amp; Scope - American Bar Association</td>
<td>249</td>
</tr>
<tr>
<td>Model Rules of Professional Conduct Rule 1.1: Competence - American Bar Association</td>
<td>254</td>
</tr>
<tr>
<td>Comment on Model Rule 1.1 - American Bar Association</td>
<td>255</td>
</tr>
<tr>
<td>Model Rules of Professional Conduct Rule 1.6: Confidentiality of Information - American Bar Association</td>
<td>257</td>
</tr>
<tr>
<td>Comment on Model Rule 1.6 - American Bar Association</td>
<td>258</td>
</tr>
<tr>
<td>Model Rules of Professional Conduct Rule 1.11: Special Conflicts of Interest for Former &amp; Current Government Officers &amp; Employees - American Bar Association</td>
<td>265</td>
</tr>
<tr>
<td>Comment on Model Rule 1.11 - American Bar Association</td>
<td>267</td>
</tr>
<tr>
<td>Model Rules of Professional Conduct Rule 1.13: Organization as Client - American Bar Association</td>
<td>270</td>
</tr>
<tr>
<td>Comment on Model Rule 1.13 - American Bar Association</td>
<td>272</td>
</tr>
<tr>
<td>The National Security Lawyer (Excerpt from ‘In the Common Defense’) - James E. Baker</td>
<td>283</td>
</tr>
<tr>
<td>Ethical Issues of the Practice of National Security Law: Some Observations - Charles J. Dunlap, Jr.</td>
<td>293</td>
</tr>
</tbody>
</table>
Panel IV:

International Organized Crime and National Security

Moderator:
John Norton Moore
STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME

Addressing Converging Threats to National Security

JULY 2011
Transnational organized crime refers to those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. There is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures. The crimes they commit also vary. Transnational organized criminals act conspiratorially in their criminal activities and possess certain characteristics which may include, but are not limited to:

- In at least part of their activities they commit violence or other acts which are likely to intimidate, or make actual or implicit threats to do so;
- They exploit differences between countries to further their objectives, enriching their organization, expanding its power, and/or avoiding detection/apprehension;
- They attempt to gain influence in government, politics, and commerce through corrupt as well as legitimate means;
- They have economic gain as their primary goal, not only from patently illegal activities but also from investment in legitimate businesses; and
- They attempt to insulate both their leadership and membership from detection, sanction, and/or prosecution through their organizational structure.
THE WHITE HOUSE
WASHINGTON

July 19, 2011

In the National Security Strategy, I committed my Administration to the pursuit of four enduring national interests: security, prosperity, respect for universal values, and the shaping of an international order that can meet the challenges of the 21st century. The expanding size, scope, and influence of transnational organized crime and its impact on U.S. and international security and governance represent one of the most significant of those challenges.

During the past 15 years, technological innovation and globalization have proven to be an overwhelming force for good. However, transnational criminal organizations have taken advantage of our increasingly interconnected world to expand their illicit enterprises.

Criminal networks are not only expanding their operations, but they are also diversifying their activities, resulting in a convergence of transnational threats that has evolved to become more complex, volatile, and destabilizing. These networks also threaten U.S. interests by forging alliances with corrupt elements of national governments and using the power and influence of those elements to further their criminal activities. In some cases, national governments exploit these relationships to further their interests to the detriment of the United States.

Despite a long and successful history of dismantling criminal organizations and developing common international standards for cooperation against transnational organized crime, not all of our capabilities have kept pace with the expansion of 21st century transnational criminal threats. Therefore, this strategy is organized around a single, unifying principle: to build, balance, and integrate the tools of American power to combat transnational organized crime and related threats to our national security — and to urge our partners to do the same. To this end, this strategy sets out 56 priority actions, starting with ones the United States can take within its own borders to lessen the impact of transnational crime domestically and on our foreign partners. Other actions seek to enhance our intelligence, protect the financial system and strategic markets, strengthen interdiction, investigations, and prosecutions, disrupt the drug trade and its facilitation of other transnational threats, and build international cooperation.

While this Strategy is intended to assist the United States Government in combating transnational crime, it also serves as an invitation for enhanced international cooperation. We encourage our partners and allies to echo the commitment we have made here and join in building a new framework for international cooperation to protect all our citizens from the violence, harm, and exploitation wrought by transnational organized crime.

Sincerely,

[Signature]
Table of Contents

Executive Summary ........................................... 1

I. Introduction .................................................. 3


III. Strategy to Combat Transnational Organized Crime. ........................................... 13

Priority Actions:

Start at Home: Taking Shared Responsibility for Transnational Organized Crime. ........ 15

Enhance Intelligence and Information Sharing. ......................................................... 17

Protect the Financial System and Strategic Markets against Transnational Organized Crime . 20

Strengthen Interdiction, Investigations, and Prosecutions ........................................ 22

Disrupt Drug Trafficking and Its Facilitation of Other Transnational Threats. ............... 24

Build International Capacity, Cooperation, and Partnerships .................................. 26
Executive Summary

The Strategy to Combat Transnational Organized Crime applies all elements of national power to protect citizens and U.S. national security interests from the convergence of 21st-century transnational criminal threats. This Strategy is organized around a single unifying principle: to build, balance, and integrate the tools of American power to combat transnational organized crime and related threats to national security—and to urge our foreign partners to do the same. The end-state we seek is to reduce transnational organized crime (TOC) from a national security threat to a manageable public safety problem in the United States and in strategic regions around the world. The Strategy will achieve this end-state by pursuing five key policy objectives:

1. Protect Americans and our partners from the harm, violence, and exploitation of transnational criminal networks.

2. Help partner countries strengthen governance and transparency, break the corruptive power of transnational criminal networks, and sever state-crime alliances.


4. Defeat transnational criminal networks that pose the greatest threat to national security by targeting their infrastructures, depriving them of their enabling means, and preventing the criminal facilitation of terrorist activities.

5. Build international consensus, multilateral cooperation, and public-private partnerships to defeat transnational organized crime.

The Strategy also introduces new and innovative capabilities and tools, which will be accomplished by prioritizing within the resources available to affected departments and agencies.

A new Executive Order will establish a sanctions program to block the property of and prohibit transactions with significant transnational criminal networks that threaten national security, foreign policy, or economic interests.

A proposed legislative package will enhance the authorities available to investigate, interdict, and prosecute the activities of top transnational criminal networks.

A new Presidential Proclamation under the Immigration and Nationality Act (INA) will deny entry to transnational criminal aliens and others who have been targeted for financial sanctions.

A new rewards program will replicate the success of narcotics rewards programs in obtaining information that leads to the arrest and conviction of the leaders of transnational criminal organizations that pose the greatest threats to national security.

An interagency Threat Mitigation Working Group will identify those TOC networks that present a sufficiently high national security risk and will ensure the coordination of all elements of national power to combat them.
I. Introduction

"Combating transnational criminal and trafficking networks requires a multidimensional strategy that safeguards citizens, breaks the financial strength of criminal and terrorist networks, disrupts illicit trafficking networks, defeats transnational criminal organizations, fights government corruption, strengthens the rule of law, bolsters judicial systems, and improves transparency. While these are major challenges, the United States will be able to devise and execute a collective strategy with other nations facing the same threats."

— National Security Strategy, May 2010

In January 2010, the United States Government completed a comprehensive review of international organized crime—the first on this topic since 1995. Based on the review and subsequent reporting, the Administration has concluded that, in the intervening years, international—or transnational—organized crime has expanded dramatically in size, scope, and influence and that it poses a significant threat to national and international security. In light of the review’s findings, we have adopted the term “transnational organized crime” (TOC) to describe the threats addressed by this Strategy. While the term “international organized crime” has been commonly used in the past, “transnational organized crime” more accurately describes the converging threats we face today. As emphasized in the National Security Strategy: “…these threats cross borders and undermine the stability of nations, subverting government institutions through corruption and harming citizens worldwide.”

In years past, TOC was largely regional in scope, hierarchically structured, and had only occasional links to terrorism. Today’s criminal networks are fluid, striking new alliances with other networks around the world and engaging in a wide range of illicit activities, including cybercrime and providing support for terrorism. Virtually every transnational criminal organization and its enterprises are connected and enabled by information systems technologies, making cybercrime a substantially more important concern. TOC threatens U.S. interests by taking advantage of failed states or contested spaces; forging alliances with corrupt foreign government officials and some foreign intelligence services; destabilizing political, financial, and security institutions in fragile states; undermining competition in world strategic markets; using cyber technologies and other methods to perpetrate sophisticated frauds; creating the potential for the transfer of weapons of mass destruction (WMD) to terrorists; and expanding narco-trafficking and human and weapons smuggling networks. Terrorists and insurgents increasingly are turning to criminal networks to generate funding and acquire logistical support. TOC also threatens the interconnected trading, transportation, and transactional systems that move people and commerce throughout the global economy and across our borders.

In October 2010, the national security advisors of 44 nations gathered in Sochi, Russia to discuss transnational crime. Representing the United States, former National Security Advisor General James L. Jones, USMC, Ret. warned of the TOC threats to international security and urged immediate international action, saying:
“In a world full of transnational threats, transnational crime is in an ascendant phase... This lethal nexus of organized crime, narco-trafficking, and terrorism is a threat that the United States, Russia and all of us share and should be working together to combat... Today, right now, we have an opportunity for cooperation not just between the United States and Russia, but among all nations represented here today. It's up to us to seize the moment...”

The various elements of this Strategy flow from a single unifying principle: we will build, balance, and integrate the tools of American power to combat TOC and related threats to national security and urge our foreign partners to do the same. To this end, the Strategy recognizes TOC as a significant threat to national and international security and emphasizes U.S. planning, priorities, and activities accordingly. The Strategy addresses TOC and drug trafficking as increasingly intertwined threats to maximize the impact of U.S. resources. It also provides a framework to direct U.S. power against those TOC actors, activities, and networks that are determined to pose the greatest threat to national and international security.

This Strategy establishes priority actions in several key areas. It starts by taking a hard look at what actions the United States can take within its own borders to lessen the threat and impact of TOC domestically and on our foreign partners. The other priority actions seek to:

- Enhance Intelligence and Information Sharing;
- Protect the Financial System and Strategic Markets Against Transnational Organized Crime;
- Strengthen Interdiction, Investigations, and Prosecutions;
- Disrupt Drug Trafficking and Its Facilitation of Other Transnational Threats; and
- Build International Capacity, Cooperation, and Partnerships.

This Strategy complements but does not replicate the work of other major U.S. security initiatives. It is guided by the National Security Strategy and interlocks with other U.S. strategies and initiatives, to include the National Drug Control Strategy, the National Strategy for Counterterrorism, the International Strategy for Cyberspace, the National Strategy to Combat Weapons of Mass Destruction, the U.S.-Mexico Merida Initiative, the Law Enforcement Strategy to Combat International Organized Crime, the National Strategy for Maritime Security, Countering Piracy Off the Horn of Africa: Partnership & Action Plan, and several other U.S. security assistance, counterdrug, and capacity-building efforts around the world.

The Interagency Policy Committee (IPC) on Illicit Drugs and Transnational Criminal Threats will oversee a whole-of-government approach to implementing this Strategy. Co-chaired by the National Security Staff and the Office of National Drug Control Policy, this IPC will issue implementation guidance, establish performance measures, and receive regular progress updates from the interagency community. This IPC will be informed by and work with other IPCs such as the Maritime Security IPC. With a new Strategy to Combat Transnational Organized Crime and an array of new authorities and tools, this Administration is committing itself to ensuring that we rise to the national security challenges of the 21st century and ensure an international order that protects the safety and well-being of our citizens.
II. Transnational Organized Crime: A Growing Threat to National and International Security

Transnational organized crime (TOC) poses a significant and growing threat to national and international security, with dire implications for public safety, public health, democratic institutions, and economic stability across the globe. Not only are criminal networks expanding, but they also are diversifying their activities, resulting in the convergence of threats that were once distinct and today have explosive and destabilizing effects. This Strategy organizes the United States to combat TOC networks that pose a strategic threat to Americans and to U.S. interests in key regions.

Penetration of State Institutions, Corruption, and Threats to Governance. Developing countries with weak rule of law can be particularly susceptible to TOC penetration. TCC penetration of states is deepening, leading to co-option in a few cases and further weakening of governance in many others. The apparent growing nexus in some states among TOC groups and elements of government—including intelligence services—and high-level business figures represents a significant threat to economic growth and democratic institutions. In countries with weak governance, there are corrupt officials who turn a blind eye to TOC activity. TOC networks insinuate themselves into the political process in a variety of ways. This is often accomplished through direct bribery (but also by having members run for office); setting up shadow economies; infiltrating financial and security sectors through coercion or corruption; and positioning themselves as alternate providers of governance, security, services, and livelihoods. As they expand, TOC networks may threaten stability and undermine free markets as they build alliances with political leaders, financial institutions, law enforcement, foreign intelligence, and security agencies. TOC penetration of governments is exacerbating corruption and undermining governance, rule of law, judicial systems, free press, democratic institution-building, and transparency. Further, events in Somalia have shown how criminal control of territory and piracy ransoms generate significant sums of illicit revenue and promote the spread of government instability.

Threats to the Economy, U.S. Competitiveness, and Strategic Markets. TOC threatens U.S. economic interests and can cause significant damage to the world financial system through its subversion, exploitation, and distortion of legitimate markets and economic activity. U.S. business leaders worry that U.S. firms are being put at a competitive disadvantage by TOC and corruption, particularly in emerging markets where many perceive that rule of law is less reliable. The World Bank estimates about $1 trillion is spent each year to bribe public officials, causing an array of economic distortions and damage to legitimate economic activity. The price of doing business in countries affected by TOC is also rising as companies budget for additional security costs, adversely impacting foreign direct investment in many parts of the world. TOC activities can lead to disruption of the global supply chain, which in turn diminishes economic competitiveness and impacts the ability of U.S. industry and transportation sectors to be resilient in the face of such disruption. Further, transnational criminal organizations, leveraging their relationships with state-owned entities, industries, or state-allied actors, could gain influence over key
commodities markets such as gas, oil, aluminum, and precious metals, along with potential exploitation of the transportation sector.

**Crime-Terror-Insurgency Nexus.** Terrorists and insurgents increasingly are turning to TOC to generate funding and acquire logistical support to carry out their violent acts. The Department of Justice reports that 29 of the 63 organizations on its FY 2010 Consolidated Priority Organization Targets list, which includes the most significant international drug trafficking organizations (DTOs) threatening the United States, were associated with terrorist groups. Involvement in the drug trade by the Taliban and the Revolutionary Armed Forces of Colombia (FARC) is critical to the ability of these groups to fund terrorist activity. We are concerned about Hizballah’s drug and criminal activities, as well as indications of links between al-Qa’ida in the Lands of the Islamic Maghreb and the drug trade. Further, the terrorist organization al-Shabaab has engaged in criminal activities such as kidnapping for ransom and extortion, and may derive limited fees from extortion or protection of pirates to generate funding for its operations. While the crime-terror nexus is still mostly opportunistic, this nexus is critical nonetheless, especially if it were to involve the successful criminal transfer of WMD material to terrorists or their penetration of human smuggling networks as a means for terrorists to enter the United States.

**Expansion of Drug Trafficking.** Despite demonstrable counterdrug successes in recent years, particularly against the cocaine trade, illicit drugs remain a serious threat to the health, safety, security, and financial well-being of Americans. The demand for illicit drugs, both in the United States and abroad, fuels the power, impunity, and violence of criminal organizations around the globe. Mexican DTOs are escalating their violence to consolidate their market share within the Western Hemisphere, protect their operations in Mexico, and expand their reach into the United States. In West Africa, Latin American cartels are exploiting local criminal organizations to move cocaine to Western Europe and the Middle East. There have also been instances of Afghan DTOs operating with those in West Africa to smuggle heroin to Europe and the United States. Many of the well-established organized criminal groups that had not been involved in drug trafficking—including those in Russia, China, Italy, and the Balkans—are now establishing ties to drug producers to develop their own distribution networks and markets. The expansion of drug trafficking is often accompanied by dramatic increases in local crime and corruption, as the United Nations has detected in regions such as West Africa and Central America.

**Human Smuggling.** Human smuggling is the facilitation, transportation, attempted transportation, or illegal entry of a person or persons across an international border, in violation of one or more countries’ laws, either clandestinely or through deception, whether with the use of fraudulent documents or through the evasion of legitimate border controls. It is a criminal commercial transaction between willing parties who go their separate ways once they have procured illegal entry into a country. The vast majority of people who are assisted in illegally entering the United States and other countries are smuggled, rather than trafficked. International human smuggling networks are linked to other transnational crimes including drug trafficking and the corruption of government officials. They can move
criminals, fugitives, terrorists, and trafficking victims, as well as economic migrants. They undermine the sovereignty of nations and often endanger the lives of those being smuggled. In its 2010 report The Globalization of Crime: A Transnational Organized Crime Threat Assessment, the United Nations Office on Drugs and Crime (UNODC) estimated that the smuggling of persons from Latin America to the United States generated approximately $6.6 billion annually in illicit proceeds for human smuggling networks.

**Trafficking in Persons.** Trafficking in Persons (TIP), or human trafficking, refers to activities involved when one person obtains or holds another person in compelled service, such as involuntary servitude, slavery, debt bondage, and forced labor. TIP specifically targets the trafficked person as an object of criminal exploitation—often for labor exploitation or sexual exploitation purposes—and trafficking victims are frequently physically and emotionally abused. Although TIP is generally thought of as an international crime that involves the crossing of borders, TIP victims can also be trafficked within their own countries. Traffickers can move victims between locations within the same country and often sell them to other trafficking organizations.

**Weapons Trafficking.** Criminal networks and illicit arms dealers also play important roles in the black markets from which terrorists and drug traffickers procure some of their weapons. As detailed in the 2010 UNODC report The Globalization of Crime, “The value of the documented global authorized trade in firearms has been estimated at approximately $1.58 billion in 2006, with unrecorded but licit transactions making up another $100 million or so. The most commonly cited estimate for the size of the illicit market is 10% - 20% of the licit market.” According to the head of UNODC, these “illicit arms fuel the violence that undermines security, development and justice” worldwide. U.S. Federal law enforcement agencies have intercepted large numbers of weapons or related items being smuggled to China, Russia, Mexico, the Philippines, Somalia, Turkmenistan, and Yemen in the last year alone.

**Intellectual Property Theft.** TOC networks are engaged in the theft of critical U.S. intellectual property, including through intrusions into corporate and proprietary computer networks. Theft of intellectual property ranges from movies, music, and video games to imitations of popular and trusted brand names, to proprietary designs of high-tech devices and manufacturing processes. This intellectual property theft causes significant business losses, erodes U.S. competitiveness in the world marketplace, and in many cases threatens public health and safety. Between FY 2003 and FY 2010, the yearly domestic value of customs seizures at U.S. port and mail facilities related to intellectual property right (IPR) violations leaped from $94 million to $188 million. Products originating in China accounted for 66% of these IPR seizures in FY 2010.

**Cybercrime.** TOC networks are increasingly involved in cybercrime, which costs consumers billions of dollars annually, threatens sensitive corporate and government computer networks, and undermines worldwide confidence in the international financial system. Through cybercrime, transnational criminal organizations pose a significant threat to financial and trust systems—banking, stock markets, e-currency, and value and credit card services—on which the world economy depends. For example, some estimates indicate that online frauds perpetrated by Central European cybercrime networks have defrauded U.S. citizens or entities of approximately $1 billion in a single year. According to the U.S. Secret Service, which investigates cybercrimes through its 31 Electronic Crimes Task Forces, financial crimes facilitated by anonymous online criminal fora result in billions of dollars in losses to the Nation's
financial infrastructure. The National Cyber Investigative Joint Task Force, led by the Federal Bureau of Investigation (FBI), functions as a domestic focal point for 18 federal departments or agencies to coordinate, integrate, and share information related to cyber threat investigations, as well as make the Internet safer by pursuing terrorists, spies, and criminals who seek to exploit U.S. systems. Pervasive criminal activity in cyberspace not only directly affects its victims, but can imperil citizens' and businesses' faith in these digital systems, which are critical to our society and economy. Computers and the Internet play a role in most transnational crimes today, either as the target or the weapon used in the crime. The use of the Internet, personal computers, and mobile devices all create a trail of digital evidence. Often the proper investigation of this evidence trail requires highly trained personnel. Crimes can occur more quickly, but investigations proceed more slowly due to the critical shortage of investigators with the knowledge and expertise to analyze ever increasing amounts of potential digital evidence.

The Critical Role of Facilitators. Connecting these converging threats are “facilitators,” semi-legitimate players such as accountants, attorneys, notaries, bankers, and real estate brokers, who cross both the licit and illicit worlds and provide services to legitimate customers, criminals, and terrorists alike. The range of licit-illicit relationships is broad. At one end, criminals draw on the public reputations of licit actors to maintain facades of propriety for their operations. At the other end are “specialists” with skills or resources who have been completely subsumed into the criminal networks. For example, TOC networks rely on industry experts, both witting and unwitting, to facilitate corrupt transactions and to create the necessary infrastructure to pursue their illicit schemes, such as creating shell corporations, opening offshore bank accounts in the shell corporation’s name, and creating front businesses for their illegal activity and money laundering. Business owners or bankers are enlisted to launder money, and employees of legitimate companies are used to conceal smuggling operations. Human smugglers, human traffickers, arms traffickers, drug traffickers, terrorists, and other criminals depend on secure transportation networks and safe locations from which to stage smuggling activity or to store bulk cash or narcotics for transport. They also depend on fraudulently created or fraudulently obtained documents, such as passports and visas, to move themselves or their clients into the United States and illegally reside here.

Transnational criminal networks such as organized crime groups, drug traffickers, and weapons dealers at times share convergence points—places, businesses, or people—to “launder” or convert their illicit profits into legitimate funds. Many of these disparate networks also appear to use the same casinos, financial intermediaries, and front companies to plan arms and narcotics deals because they view them as safe intermediaries for doing business. Cash-intensive and high-volume businesses such as casinos are especially attractive, particularly those in jurisdictions that lack the political will and oversight to regulate casino operations or fail to perform due diligence on casino licensees. Illicit networks similarly abuse some of the same financial intermediaries and front companies in regions where government or law enforcement corruption is prevalent, with officials receiving either revenues from the criminal businesses or ownership stakes in the legitimate-appearing commercial entity.
Regional Priorities

TOC—a global problem—manifests itself in various regions in different ways.

Western Hemisphere: TOC networks—including transnational gangs—have expanded and matured, threatening the security of citizens and the stability of governments throughout the region, with direct security implications for the United States. Central America is a key area of converging threats where illicit trafficking in drugs, people, and weapons—as well as other revenue streams—fuel increased instability. Transnational crime and its accompanying violence are threatening the prosperity of some Central American states and can cost up to eight percent of their gross domestic product, according to the World Bank. The Government of Mexico is waging an historic campaign against transnational criminal organizations, many of which are expanding beyond drug trafficking into human smuggling and trafficking, weapons smuggling, bulk cash smuggling, extortion, and kidnapping for ransom. TOC in Mexico makes the U.S. border more vulnerable because it creates and maintains illicit corridors for border crossings that can be employed by other secondary criminal or terrorist actors or organizations. Farther south, Colombia has achieved remarkable success in reducing cocaine production and countering illegal armed groups, such as the FARC, that engage in TOC. Yet, with the decline of these organizations, new groups are emerging such as criminal bands known in Spanish as Bandas Criminales, or Bacrim.

Colombia: From Recipient to Provider of Assistance

After years of intensive capacity building assistance in Colombia, the United States is working to transfer financial and operational responsibility for institutional development to the Government of Colombia. Colombia is working to expand, improve, and develop new partnerships, providing assistance and advice for police, prosecutors, protection programs, and judiciary, criminal law, and procedure development. This reality is the result of the success of U.S. assistance to Colombia. Capacity building is success. The United States aims to replicate with other partner states. On July 2, 2006, the world witnessed the extraordinary courage and capability of Colombian forces during the daring rescue of 3 hostages—including 3 Americans—who had been held captive for years in the jungles by FARC guerrillas. The rescue was accomplished without firing a shot.

Afghanistan/Southwest Asia: Nowhere is the convergence of transnational threats more apparent than in Afghanistan and Southwest Asia. The Taliban and other drug-funded terrorist groups threaten the efforts of the Islamic Republic of Afghanistan, the United States, and other international partners to build a peaceful and democratic future for that nation. The insurgency is seen in some areas of Afghanistan as criminally driven—as opposed to ideologically motivated—and in some areas, according to local Afghan officials and U.S. estimates, drug traffickers and the Taliban are becoming indistinguishable. In other instances, ideologically
driven insurgent networks are either directly trafficking in narcotics or have linked up with DTOs to finance their criminal actions. The threatening crime-terror-insurgency nexus in this region is illustrated by cases such as that of INTERPOL fugitive Dawood Ibrahim, the reputed leader of South Asia's powerful "D Company." He is wanted in connection with the 1993 Mumbai bombing and is sanctioned under United Nations Security Council Resolution 1267 (Taliban/al-Qa'ida).

**Russia/Eurasia:** Russian and Eurasian organized crime networks represent a significant threat to economic growth and democratic institutions. Russian organized crime syndicates and criminally linked oligarchs may attempt to collude with state or state-allied actors to undermine competition in strategic markets such as gas, oil, aluminum, and precious metals. At the same time, TOC networks in the region are establishing new ties to global drug trafficking networks. Nuclear material trafficking is an especially prominent concern in the former Soviet Union. The United States will continue to cooperate with Russia and the nations of the region to combat illicit drugs and TOC.

**The Balkans:** A traditional conduit for smuggling between east and west, the Balkans has become an ideal environment for the cultivation and expansion of TOC. Weak institutions in Albania, Kosovo, and Bosnia and Herzegovina have enabled Balkan-based TOC groups to seize control of key drug and human trafficking routes and Western European markets. The Balkans region has become a new entry point for Latin American cocaine, a source of synthetic drugs, and a transit region for heroin chemical precursors for use in the Caucasus and Afghanistan. Excess weapons are smuggled to countries of concern. Insufficient border controls and the ease of acquiring passports enable the transit of criminals and terrorist figures to Western Europe. Cooperation between the United States and the European Union, as well as bilateral cooperation with the countries in the region to foster legal institution building, economic progress, and good governance in the Balkans will be key to eliminating the environment supporting TOC.

**West Africa:** West Africa has become a major transit point for illegal drug shipments to Europe and for Southwest Asian heroin to the United States. It has also become both a source of—and transit point for—methamphetamine destined for the Far East. West Africa also serves as a transit route for illicit proceeds flowing back to source countries. TOC exacerbates corruption and undermines the rule of law, democratic processes, and transparent business practices in several African states that already suffer from weak institutions. Due to its lack of law enforcement capabilities, its susceptibility to corruption, its porous borders, and its strategic location, Guinea-Bissau remains a significant hub of narcotics trafficking on the verge of developing into a narco-state. While many officials within the Government of Guinea-Bissau recognize the extent of the drug problem and express a willingness to address it, a crippling lack of resources and capacity remains a hindrance to real progress in combating drug trafficking. The recent re-appointment of U.S. Treasury-designated drug kingpin Jose Americo Bubo Na Tchuto as Naval Chief of Staff is likely to further entrench drug cartels in the permissive operating conditions prevailing in Guinea-Bissau. In the Gulf of Guinea, maritime criminals operate in areas of weak governance, kidnapping oil workers, stealing oil from pipelines, and causing environmental damage that harms the citizenry. The United States will work with African governments, European partners, and multilateral institutions to counter this threat to development, democratic processes, and the rule of law in the region.
Asia/Pacific: TOC networks and DTOs are integrating their activities in the Asia/Pacific region. Due to the region's global economic ties, these criminal activities have serious implications worldwide. The economic importance of the region also heightens the threat posed to intellectual property rights, as a large portion of intellectual property theft originates from China and Southeast Asia. Human trafficking and smuggling remain significant concerns in the Asia/Pacific region, as demonstrated by the case of convicted alien smuggler Cheng Chui Ping, who smuggled more than 1,000 aliens into the United States during the course of her criminal career, sometimes hundreds at a time. TOC networks in the region are also active in the illegal drug trade, trafficking precursor chemicals for use in illicit drug production. North Korean government entities have likely maintained ties with established crime networks, including those that produce counterfeit U.S. currency, threatening the global integrity of the U.S. dollar. It is unclear whether these links persist. The United States will continue to improve its understanding of the TOC threats in the Asia/Pacific region and will work with partner nations to develop a comprehensive response.
III. Strategy to Combat Transnational Organized Crime

For decades, the United States and other countries have dismantled scores of criminal organizations around the world. The U.S. experience with La Cosa Nostra, as well as Colombia’s experience with the Medellín and Cali Cartels—and even the FARC—prove that it is possible to constrain, shrink, disrupt and dismantle criminal and insurgent groups once considered to be untouchable.

This Strategy builds upon such past experience. Today the threat from TOC is more complicated because criminal networks are more fluid and are using increasingly sophisticated tactics. TOC can exploit the interconnected nature of our modern trading, transportation, and transnational systems that move people and commerce throughout the global economy and across our borders. Countering TOC today requires an integrated and comprehensive approach. This Strategy sets out such an approach to raise international awareness about the reality of the TOC threat to international security; galvanize multilateral action to constrain the reach and influence of TOC; deprive TOC of its enabling means and infrastructure; shrink the threat TOC poses to citizen safety, national security, and governance; and ultimately defeat the TOC networks that pose the greatest threat to national security. TOC presents sophisticated and multifaceted threats that cannot be addressed through law enforcement action alone. Accordingly, we will establish an interagency Threat Mitigation Working Group to identify those TCC networks that present a sufficiently high national security threat as to merit the focused use of complementary law enforcement and non-law enforcement assets and that may be vulnerable to whole-of-government responses. The Working Group will ensure the coordination of all elements of national power to effectively protect our borders, people, economy, and financial system from the threats posed by the most dangerous and sophisticated of these transnational criminal networks.

This Strategy sets out five overarching policy objectives that are consistent with the vision and priorities of the National Security Strategy:

1. Protect Americans and our partners from the harm, violence, and exploitation of transnational criminal networks. Our priority is the safety, security, and prosperity of American citizens and the citizens of partner nations. We will target the networks that pose the gravest threat to citizen safety and security, including those that traffic illicit drugs, arms, and people—especially women and children; sell and distribute substandard, tainted and counterfeit goods; rob Americans of their prosperity; carry out kidnappings for ransom and extortion; and seek to terrorize and intimidate through acts of torture and murder.

2. Help partner countries strengthen governance and transparency, break the corruptive power of transnational criminal networks, and sever state-crime alliances. The United States needs willing, reliable and capable partners to combat the corruption and instability generated by TOC and related threats to governance. We will help international partners develop the sustainable capacities necessary to defeat transnational threats; strengthen legitimate and effective public safety, security, and justice institutions; and promote universal values. We will also seek to sever
the powerful strategic alliances that form between TOC and states, including those between TOC networks and foreign intelligence services.

3. **Break the economic power of transnational criminal networks and protect strategic markets and the U.S. financial system from TOC penetration and abuse.** TOC networks—using bribery, fraud, and violence—have the capacity to disrupt economic activity and put legitimate businesses at a distinct competitive disadvantage. We will attack the financial underpinnings of the top transnational criminals; strip them of their illicit wealth; sever their access to the financial system; expose their criminal activities hidden behind legitimate fronts; and protect strategic markets and the U.S. financial system.

4. **Defeat transnational criminal networks that pose the greatest threat to national security, by targeting their infrastructures, depriving them of their enabling means, and preventing the criminal facilitation of terrorist activities.** We will target, disrupt, and defeat the TOC networks that pose the greatest threat to the safety and security of Americans and U.S. national security interests. These include criminal networks—including transnational criminal gangs—that traffic drugs, bulk cash, arms, people, sensitive documents, or other contraband. Further, we will seek to prevent collaboration between criminal and terrorist networks and deprive them of their critical resources and infrastructure, such as funding, logistical support for transportation, staging, procurement, safe havens for illicit activities, and the facilitation of services and materiel, which could include WMD material.

5. **Build international consensus, multilateral cooperation, and public-private partnerships to defeat transnational organized crime.** We will build new partnerships—with industry, finance, academia, civil society and non-governmental organizations—to combat TOC networks that operate in the illicit and licit worlds. We will also fight criminal networks with an alliance of legitimate networks, and ensure the freedom of the press so that the media and journalists may safely expose the harms inflicted by TOC. We will expand and deepen our understanding, cooperation, and information sharing at home with State and local agencies, with foreign partners, and with multilateral institutions. Internationally, we will further international norms against tolerating or sponsoring crime in all its forms, including in cyberspace.
Priority Actions

Start at Home: Taking Shared Responsibility for Transnational Organized Crime

I reiterated that the United States accepts our shared responsibility for the drug-violence. So to combat the southbound flow of guns and money, we are screening all southbound rail cargo, seizing many more guns bound for Mexico, and we are putting more gunrunners behind bars. And as part of our new drug control strategy, we are focused on reducing the demand for drugs through education, prevention and treatment... We are very mindful that the battle President Calderón is fighting inside of Mexico is not just his battle; it's also ours. We have to take responsibility just as he's taking responsibility.

—President Barack Obama speaking at a joint press conference with Mexican President Felipe Calderón, March 3, 2011

We must begin our effort to disrupt TOC by looking inward and acknowledging the causes that emanate from within our own borders to fuel and empower TOC. The demand for illegal drugs within the United States fuels a significant share of the global drug trade, which is a primary funding source for TOC networks and a key source of revenue for some terrorist and insurgent networks. Any comprehensive strategy to defeat TOC must seek to reduce the demand for drugs and other illegal goods that finance TOC networks. The President's National Drug Control Strategy emphasizes prevention, early intervention, treatment, and innovative criminal justice approaches to drive down drug use, and calls for continued support for the millions of Americans who are in recovery from addiction. Supported by a budget that increases resources for vital prevention and treatment programs, the National Drug Control Strategy seeks to reduce the size of the illegal drug market in the United States, depriving TOC networks of revenue while helping more of our citizens break the cycle of drug abuse and reducing the adverse consequences to our communities.

We must also stop the illicit flow from the United States of weapons and criminal proceeds that empower TOC networks. The Administration has placed an increased emphasis on stemming these outbound flows, dedicating additional law enforcement, investigative, and prosecution resources to targeting TOC, such as deploying additional U.S. Customs and Border Protection "outbound teams" to our borders, screening outbound rail and vehicle traffic for weapons and bulk currency, and by investing additional resources in the integrated Border Enforcement Security Task Forces along the U.S.-Mexico border to investigate the organizations involved in cross-border crimes. We will also work with Congress to seek ratification or accession to key multilateral instruments related to countering the illicit trafficking of weapons.

Further, we will work with our international partners to build their law enforcement capacities, strengthen their judicial institutions, and combat the corrosive threat of corruption, while also recognizing that the United States itself is not immune to public corruption. Continued vigilance is required to ensure the integrity of U.S. officials and institutions as we face the new and converging threats posed by TOC. In
addition to the greater vigilance required by our governmental institutions, American businesses and individuals need to inform law enforcement about criminal activity and reduce their vulnerability to fraud schemes, intellectual property theft, and identity theft. Acknowledging our own challenges and aggressively addressing them here at home represent the first essential steps in building the cooperative multilateral approach required to defeat TOC.

**Actions**

A. Reduce the demand for illicit drugs in the United States, thereby denying funding to illicit trafficking organizations.

B. Continue to attack drug trafficking and distribution networks and their enabling means within the United States to reduce the availability of illicit drugs.

C. Sever the illicit flow across U.S. borders of people, weapons, currency, and other illicit finance through investigations and prosecutions of key TOC leadership, as well as through the targeting of TOC networks' enabling means and infrastructure.

D. Identify and take action against corporate and governmental corruption within the United States.

E. Work with Congress to secure ratification of the Inter American Convention against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives and Other Related Materials.

F. Seek accession to the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, supplementing the UN Convention against Transnational Organized Crime.

---

**Project Deliverance: Targeting Mexican Drug Trafficking Networks in the United States**

On June 5, 2010 the DEA-led interagency Project Deliverance Operations Division executed a coordinated takedown. In support of Project Deliverance a 22 month multi-agency network of law enforcement investigations targeting the transportation infrastructure of Mexican transnational criminal organizations in the United States, especially along the Southwest border. During the final takedown, 429 arrests took place in 16 states through cooperation among more than 10,000 Federal, State, and Local law enforcement officers. In total, Project Deliverance has led to 2,562 arrests and the seizure of $94 million, 1,262 pounds of methamphetamine, 2.5 tons of cocaine, 2,110 pounds of heroin, 69 tons of marijuana, 501 weapons, and 577 vehicles during the entire course of the operation.
Enhance Intelligence and Information Sharing

A shift in U.S. intelligence collection priorities since the September 11, 2001 attacks left significant gaps in TOC-related intelligence. Meanwhile, the TOC threat has worsened and grown in complexity over the past 15 years. The fluid nature of TOC networks, which includes the use of criminal facilitators, makes targeting TOC increasingly difficult.

Enhancing U.S. intelligence collection, analysis, and counterintelligence on TOC is a necessary first step, but should be accompanied by collaboration with law enforcement authorities at Federal, State, local, tribal, and territorial levels and enhanced sharing with foreign counterparts. We will also supplement our understanding of TOC involvement in licit commercial sectors to better enable policymakers to develop specific interventions. Our aim is enhanced intelligence that is broad-based and centered on substantially upgraded signals intelligence (SIGINT), human intelligence (HUMINT) and open sources intelligence (OSINT). This effort will be aided through greater information sharing with foreign partners and closer cooperation among intelligence, law enforcement, and other applicable agencies domestically.

We will augment our intelligence in step with the new TOC threats described previously. The Administration will review its current intelligence priorities, including the National Intelligence Priorities Framework, and determine how best to enhance our intelligence against the highest-level TOC threats to national security. Priorities will include:

- Enhancing SIGINT and HUMINT collection on TOC threats, especially taking into account the potential role of TOC to facilitate WMD terrorism;
- Employing the Open Source Center to draw upon “grey” literature, smaller press outlets that cover crime in foreign countries, and social media fora to develop profiles of individuals, companies, and institutions linked to TOC networks;
- Coordinating with the interagency International Organized Crime Intelligence and Operations Center (IOC-2) to utilize existing resources and databases of the Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center (OFC) and SOD to share intelligence, de-conflict operations, and produce actionable leads for investigators and prosecutors working nationwide;
- Expanding collection and immigration, customs, transportation, and critical infrastructure screening capabilities in TOC “hotspots” around the world;
- Developing protocols to ensure appropriate TOC data flows to agencies conducting screening and interdiction operations to disrupt TOC activities at the border and at critical points of the supply chain;
- Using specialized intelligence centers such as the El Paso Intelligence Center, the Bulk Cash Smuggling Center, the National Export Enforcement Coordination Center, and the Cyber Crimes Center to coordinate the collection and analysis of intelligence regarding various aspects of the TOC threat;
- Using the National Intellectual Property Rights Coordination Center, an interagency and international law enforcement task force established in 2000 and led by ICE, to assist with combating
intellectual property theft and maintaining the integrity of public health, public safety, the military, and the U.S. economy; and

- Enhancing Department of Defense support to U.S. law enforcement through the Narcotics and Transnational Crime Support Center.

**Actions**

A. Enhance U.S. intelligence collection, analysis, and counterintelligence on TOC entities that pose the greatest threat to national security.

B. Develop greater synergies between intelligence analysts, collectors, and counterintelligence personnel; ensure their efforts directly support operational law enforcement needs and screening requirements.

C. Strengthen ties among U.S. intelligence and counterintelligence, law enforcement, and military entities, while strengthening cooperation with international intelligence and law enforcement partners.

D. Develop and foster stronger law enforcement and Intelligence Community relationships among Federal, State, local, tribal, and territorial authorities.

E. Support multilateral senior law enforcement exchanges to promote the sharing of criminal intelligence and enhance cooperation, such as the "Quintet of Attorneys-General" and the "Strategic Alliance Group" fora established with the United Kingdom, Canada, New Zealand, and Australia.

F. Update the National Intelligence Priorities Framework to ensure that it is aligned with current TOC threats.

G. Enhance support to Intelligence Community analysis of TOC by the Office of the Director of National Intelligence, specifically by the National Intelligence Council and the National Intelligence Managers.

H. The National Counterproliferation Center shall develop a plan that assesses the links between TOC and WMD proliferators.

I. Establish a comprehensive and proactive information-sharing mechanism to identify TOC actors and exclude them from the United States or uncover them within the United States.

---

**INFORMATION SHARING TO COMBAT TRANSNATIONAL ORGANIZED CRIME**

**The Special Operations Division**

Established in 1994, the Special Operations Division (SOD) is a DEA-led, multi-agency operations coordination center with participation from federal law enforcement agencies, the Department of Defense, the Intelligence Community, and international law enforcement partners. SOD's mission is to establish strategies and operations to dismantle national and international trafficking organizations by attacking their command and control communications. Special emphasis is placed on those major drug trafficking and narco-terrorism organizations that operate across jurisdictional boundaries at the national, state, and international level. SOD provides critical and domestic-based law enforcement agents with timely investigative information that enables them to fully exploit Federal law enforcement's investigative authority under Title II of the U.S. Code. SOD coordinates overlapping investigations, ensuring that tactical and operational intelligence is shared among law enforcement agencies.
The Organized Crime-Drug Enforcement Task Force Fusion Center

Created in June 2006, the Organized Crime-Drug Enforcement Task Force (OCDETF) Fusion Center (OFC) serves as a clearinghouse for drug, intelligence, financial intelligence, and related investigative information, and is designed to conduct cross-agency integration and analysis of such data with a view to creating comprehensive investigative briefs of targeted organizations, including those identified as Core Organized Priority Organization Targets—the United States' most wanted international drug and money-laundering targets. The OFC provides agencies with operational human and financial intelligence, and is staffed with agents and analysts detailed from 54 participating investigative agencies. These personnel conduct analysis to produce investigative leads, develop target profiles, and identify links between drug organizations and other criminal activity in support of drug investigations.

The International Organized Crime Intelligence and Operations Center

In May 2009, Attorney General Eric Holder announced the establishment of the International Organized Crime, Intelligence and Operations Center (IOC-2), an entity that marshals the resources and information of U.S. law enforcement agencies and federal prosecutors to collectively combat the threats posed by international criminal organizations. Understanding that international criminal organizations are profit-driven, IOC-2 also works with investigators and prosecutors to target the criminal proceeds and assets of international criminal organizations. In recognition of the demonstrated interdependence between criminal organizations that engage in illicit drug trafficking and those that engage in international organized crime involving a broader range of criminal activities, IOC-2 works in close partnership with the OFC and SDF.

The Bulk Cash Smuggling Center

ICE established the National Bulk Cash Smuggling Center (BCSC) in 2009 to combat bulk cash smuggling. The BCSC is an operations support facility providing real time investigative assistance to the Federal, State, and local officers involved in enforcement and interdiction of bulk cash smuggling and the transportation of illicit proceeds. The BCSC is partnered with the El Paso Intelligence Center to further identify and target the financial infrastructure of drug trafficking organizations. These organizations seek to avoid traditional financial institutions by repatriating illicit proceeds through commercial and private aircraft, passenger and commercial vehicles, mail and maritime vessels, and pharmaceutical couriers at our U.S. land borders. These combined interagency efforts, successful financial investigations, Bank Secrecy Act requirements, and anti-money laundering compliance by financial institutions have strengthened formal financial systems and forced criminal organizations to seek other means to transport illicit funds across our borders.

The EPIC Border Intelligence Fusion Section

The El Paso Intelligence Center (EPIC), managed by the DEA, was established in 1974 to support enforcement efforts against drug and alien smuggling along the Southwest border. EPIC has grown over time to better support federal, state, local, and tribal law enforcement. The DEA Office of Intelligence and Analysis established the Border Intelligence Fusion Section (BIFS) at EPIC in November 2016 with the objective of providing U.S. law enforcement, border enforcement, and investigative agencies with multi-source intelligence and law enforcement information to support investigations, interdictions, and other law enforcement-related operations related to the Southwest border. The BIFS is a joint, collaborative effort of the Department of Homeland Security, Department of Justice, Department of Defense, and partners in the Intelligence Community who, in a multi-source, multi-agency intelligence section that EPIC, the BIFS will access and analyze intelligence and information received by and developed at EPIC in order to produce a common intelligence picture with current operating picture.
Protect the Financial System and Strategic Markets Against Transnational Organized Crime

Transnational criminals are now more entrepreneurial and sophisticated, and their growing infiltration of licit commerce and economic activity fundamentally threatens the free markets and financial systems that are critical to the stability and efficiency of the global economy. TOC threatens free markets because it disregards the laws and norms that legitimate businesses respect, thereby reaping an unfair competitive advantage. By eroding market integrity, quality, and competitiveness and using financial systems to move, conceal, and increase illicit funds, transnational criminals exploit and undermine not only the interests of the United States but also those of all countries promoting the rule of law.

By carefully following strategic and emerging markets for indicators of criminal interest, the United States can detect, disrupt, and reduce the economic power of TOC. To do so, the United States will work with our international partners to deter or sever crime-state alliances, raise awareness to alert businesses that may be unwitting facilitators for criminal enterprises, and continue to develop appropriate safeguards to protect the legitimate flow of trade and investment. By targeting criminal assets and opportunities, the United States and its allies can markedly reduce the profitability, growth, and evolution of TOC networks.

However, some TOC activity is inherently harder to detect and deter. The United States will place special emphasis on IPR violations and cybercrimes due to their particular impact on the economy and consumer health and safety. The United States remains intent on improving the transparency of the international financial system, including an effort to expose vulnerabilities that could be exploited by terrorist and other illicit financial networks. At the same time, the United States will enhance and apply our financial tools and sanctions more effectively to close those vulnerabilities, disrupt and dismantle illicit financial networks, and apply pressure on the state entities that directly or indirectly support TOC. We will continue to monitor TOC infiltration of the global economy to better protect the financial system and freeze the assets of criminal networks under expanded Presidential sanctions authorities and/or seize them under existing forfeiture laws.

Actions
A. Implement a new Executive Order to prohibit the transactions and block the assets under U.S. jurisdiction of TOC networks and their associates that threaten critical U.S. interests.
B. Prevent or disrupt criminal involvement in emerging and strategic markets.
C. Increase awareness and provide incentives and alternatives for the private sector to reduce facilitation of TOC.
D. Develop a mechanism that would make unclassified data on TOC available to private sector partners.
E. Implement the Administration's joint strategic plan on intellectual property enforcement to target, investigate, and prosecute intellectual property crimes committed by TOC.
F. Enhance domestic and foreign capabilities to combat the increasing involvement of TOC networks in cybercrime and build international capacity to forensically exploit and judicially process digital evidence.
G. Use authorities under the USA PATRIOT Act to designate foreign jurisdictions, institutions, or classes of transactions as "primary money-laundering concerns," allowing for the introduction of various restrictive measures on financial dealings by U.S. persons with those entities.

H. Identify foreign kleptocrats who have corrupt relationships with TOC networks and target their assets for freezing, forfeiture, and repatriation to victimized governments.

I. Work with Congress to enact legislation to require disclosure of beneficial ownership information of legal entities at the time of company formation in order to enhance transparency for law enforcement and other purposes.

J. Support the work of the Financial Action Task Force, which sets and enforces global standards to combat both money laundering and the financing of terrorism.

The Mogilevich Organization

Semen Mogilevich is wanted by the United States for fraud, racketeering, and money laundering and was recently added to the FBI's Ten Most Wanted fugitives list. Mogilevich and several members of his criminal organization were charged in 2003 in the Eastern District of Pennsylvania in a 45-count racketeering indictment with involvement in a sophisticated securities fraud and money-laundering scheme, in which they allegedly used a Pennsylvania company, YBM Magnex, to defraud investors of more than $1.5 billion. Even after that indictment and being placed on the FBI's Ten Most Wanted List, Mogilevich has continued to expand his criminal empire. Mogilevich was arrested by Russian police on tax charges in January 2008 and was released pending trial in July 2009. Other members of his organization remain at large.
Strengthen Interdiction, Investigations, and Prosecutions

This Strategy sets priorities and objectives to help law enforcement and other applicable agencies at the Federal, State, local, territorial and tribal levels work together in a collaborative manner to target TOC networks—their leaders as well as their enabling means and infrastructure—in the United States and abroad. It is equally important that we build strong working relationships with our international partners to harmonize our efforts, and to ensure that they have the capabilities and regulatory and legislative frameworks to prevent, reduce, and eliminate TOC threats.

Building upon the improved information sharing described earlier, the United States will leverage consolidated TOC databases to provide more accurate intelligence on known TOC members and their associates so they can more easily be denied entry to the United States or access to lawful immigration status, employment, or secure facilities.

This Strategy pursues TOC through criminal investigations and interdiction focused on both the networks and their leadership. Criminal investigations will use an integrated approach that incorporates financial, weapons, and TOC-related corruption investigations into a comprehensive attack on the entire criminal organization. Interdiction efforts will focus on depriving TOC networks of their products, proceeds, infrastructure, and enabling means. The use of multi-agency task forces such as the ICE-led Border Enforcement Security Task Forces will remain essential to our efforts to investigate and interdict TOC threats at our borders.

To address recent TOC trends, the Administration will work with Congress on a range of legislative solutions to allow or enhance the prosecution of TOC enterprises and significant TOC activity that affects the United States. We will also enhance our anti-money laundering and forfeiture authorities to target TOC networks that pose threats to national and international security.

Actions
A. Work with Congress to enhance U.S. authorities to identify, investigate, interdict, and prosecute top transnational criminal networks.

B. Utilize rewards programs to assist in gathering information leading to the arrest or conviction of top transnational criminals.

C. Issue a new Presidential Proclamation under the Immigration and Nationality Act to refuse visas/deny entry to TOC-affiliated aliens, corrupt foreign officials, and other persons designated for financial sanctions pursuant to the International Emergency Economic Powers Act.

D. Develop a strategy that denies TOC networks and individuals in the United States access to their infrastructure and their enabling means.

E. Deny visas to TOC members and associates and capture top TOC figures who take refuge in the United States or partner countries.

F. Fully integrate financial, weapons, and TOC-related corruption investigations into comprehensive organizational attack activities and operations.
G. Strengthen cooperation with international police organizations, such as Interpol, Europol, Ameripol, and the International Association of Chiefs of Police (IACP), to facilitate cross-border police cooperation.

H. Strengthen efforts to interdict illicit trafficking in the air and maritime domains.

I. Develop and implement a whole-of-government plan to counter kidnapping for ransom in order to disrupt the funding for terrorists, pirates, and other bad actors.

J. Deny TOC access to secure facilities and locations.

---

**The U.S. Secret Service’s Cyber Intelligence Efforts**

The U.S. Secret Service leverages technology and information obtained through private partnerships to monitor developing technologies and trends in the financial payments industry. The information obtained is used to enhance the U.S. Secret Service’s capabilities to prevent and mitigate attacks against the financial and telecommunications infrastructures. This approach to intelligence collection and sharing has resulted in the successful apprehension of individuals charged with committing some of the world’s most advanced cybercrimes during such investigations as those of the Pearl and 7-11 Intrusions, Maksym Yastremskiy, Albert González, and others. In FY-2010, the U.S. Secret Service arrested four suspects for cybercrime-related violations, with a fraud loss of $507 million.

---

**Defending U.S. Borders against TOC**

In 2006, a rising crime on the Southwest border, ICE and CBP worked with other Federal, State, local, and foreign partners to establish the Border Enforcement Security Task Force (BEST™), designed to attack TOC networks that exploit our borders and threaten the American public. Since then, this initiative has grown to 21 BESTs arrayed along the Southwest and Northern borders as well as at major seaports. These BESTs have seized more than 36,000 pounds of cocaine, 500 pounds of heroin, 385,000 pounds of marijuana, 4,300 weapons, and $68 million, and led to the arrests of 5,800 individuals.
Disrupt Drug Trafficking and Its Facilitation of Other Transnational Threats

In recent years, new developments in technology and communications equipment have enabled TOC networks involved in drug trafficking and other illicit activities to plan, coordinate, and perpetrate their schemes with increased mobility and anonymity. As a result, many DTOs have developed into versatile, loose networks that cooperate intermittently but maintain their independence. They operate worldwide and employ sophisticated technology and financial savvy. These criminal networks bribe government officials and take advantage of weak border security and ill-equipped law enforcement to facilitate their operations. Along emerging trafficking routes, such as the transit route through West Africa to Europe, criminal networks are spreading corruption and undermining fledgling democratic institutions. Due to the enormous profits associated with drug trafficking, the illegal trade is also a way to finance other transnational criminal and terrorist activities.

To diminish these threats, we will continue ongoing efforts to identify and disrupt the leadership, production, intelligence gathering, transportation, and financial infrastructure of major TOC networks. By targeting the human, technology, travel, and communications aspects of these networks, we will be able to monitor and gather intelligence to identify the full scope of the TOC networks, their members, financial assets, and criminal activities. We will continue ongoing efforts to enhance collaboration among domestic law enforcement agencies and our foreign counterparts in order to strengthen our ability to coordinate investigations and share intelligence to combat drug trafficking and TOC. Continued use of economic sanctions under the Foreign Narcotics Kingpin Designation Act (Kingpin Act) to pursue transnational drug organizations will enhance our ability to disrupt and dismantle TOC networks. The Kingpin Act also may be used to prosecute persons involved in illegal activities linked to drug trafficking, such as arms trafficking, bulk cash smuggling, or gang activity. Enhanced intelligence sharing and coordination among law enforcement and intelligence agencies, the military, and our diplomatic community will enable the interagency community to develop aggressive, multi-jurisdictional approaches to dismantle TOC networks involved in drug trafficking.

The United States will continue to aggressively target the nexus among TOC networks involved in drug trafficking, terrorist groups, piracy on the high seas, and arms traffickers. In FY 2002, the DEA formally established the Counter-Narco-Terrorism Operations Center (CNTOC) within SOD, which coordinates all DEA investigations and intelligence linked to narco-terrorism and is central to U.S. efforts to disrupt these crime-terror relationships. The United States will utilize its bilateral maritime counterdrug agreements and operational procedures to facilitate cooperation in counterdrug operations. We must attack these organizations as close to the source as we can by forward deploying our law enforcement and intelligence assets. All-source intelligence is used by U.S. Coast Guard assets in the transit zone to extend our borders by interdicting and apprehending traffickers.

The United States will continue its longstanding cooperation with the international community in our joint efforts to disrupt the world drug trade through support for drug crop reduction, promotion of alternative livelihoods, and partner nation capacity building. Our counternarcotics efforts will apply all available tools to ensure that improvements are permanent and sustainable by international allies. These efforts will include complementary and comprehensive assistance programs across the prevention, intervention, and enforcement spectrum. By disrupting and dismantling the world’s major TOC
networks involved in drug trafficking, we will be able to reduce the availability of illicit drugs, inhibit terrorist funding, improve national and international security, and bring TOC networks to justice.

**Actions**

A. Work with international partners to reduce the global supply of and demand for illegal drugs and thereby deny funding to TOC networks.

B. Sever the links between the international illicit drug and arms trades, especially in strategic regions that are at risk of being destabilized by these interconnected threats.

C. Sustain pressure to disrupt Consolidated Priority Organization Targets, as they often have a particularly corrupting influence or provide support to terrorism.

D. Maximize use of the Kingpin Act to pursue transnational drug organizations.

E. Develop a comprehensive approach to dismantle DTOs with connections to terrorist organizations.

F. Work with international partners to shut down emerging drug transit routes and associated corruption in West Africa.

G. Coordinate with international partners to prevent synthetic drug production, trafficking, and precursor chemical diversion.

---

**Countering Illicit Finance for Drug Traffickers & Terrorists**

In February 2011, the U.S. Department of the Treasury, based upon an investigation by the DEA, announced the identification of the Lebanese-Cayman Bank (LCB) as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act. The U.S. Treasury determined this bank was, in essence, facilitating narcotics trafficking and money laundering activities of an international narcotics trafficking and money laundering network controlled by ‘Amine Journa’, who was designated as a drug kingpin on January 26, 2011, pursuant to the Kingpin Act. This network moved illegal drugs from South America to Europe and the Middle East via West Africa and laundered hundreds of millions of dollars through accounts held at LCB, as well as through trade-based money-laundering involving consumer goods throughout the world, including through a bank in Malaysia.

**International Drug Enforcement Conference**

The annual DEA-led International Drug Enforcement Conference (IDEC), which has been held annually for the past 28 years, is a major contributor to international cooperation and capacity building. The IDEC brings together law enforcement and senior officials from over 100 nations to a single venue where key issues are set for cooperation, intelligence sharing, and case prioritization. IDEC—the world’s largest international drug law enforcement conference—has produced concrete results year after year. During the conferences, DEA and partner nations jointly develop plans to build greater law enforcement and investigative capacity. In addition, host nation personnel and U.S. law enforcement exchange information on priority investigative targets.
Build International Capacity, Cooperation, and Partnerships

Sustainable progress against TOC requires both political commitment and effective law enforcement and criminal justice capacities on a worldwide basis. TOC threatens the security and well-being of people around the world and jeopardizes the functioning of the global economy. Not all of these threats are equally visible to international audiences. Absent broad recognition of these shared threats, our collaboration with international partners to confront TOC will be constrained by limited political will. The United States will reach out directly to the international business community and the general public to convey that both nations and individuals share a common enemy in TOC and have a common stake in addressing this threat.

For nations that have the will to fulfill their international law enforcement commitments but lack the necessary means, the United States is committed to partnering with them to develop stronger law enforcement and criminal justice institutions necessary for ensuring the rule of law. Over the past decade, important gains have been made in developing criminal justice capacities in key regions of the world. The goal of the United States is to promote the expansion of such achievements on a worldwide basis, to the point where international law enforcement capabilities and cooperation among states are self-sustaining. Great progress also has been made in developing a common normative framework for international cooperation against TOC threats. The challenge for the United States and other countries over the next decade is to bring the promise of this worldwide regime into practice. The United States will encourage international partners to dedicate the necessary political capital and resources toward making the promise of these commitments a reality. The United States will pursue this through both a renewed commitment to multilateral diplomacy and by leveraging bilateral partnerships to elevate the importance of combating TOC as a key priority of U.S. diplomacy. For example, in February 2011, the United States and the United Kingdom established the Organized Crime Contact Group, to be chaired by the UK Home Secretary and the Assistant to the President for Homeland Security and Counterterrorism. In addition, the United States deploys hundreds of law enforcement attaches to its missions abroad to develop and maintain foreign contacts essential to combating immediate threats to public safety and security. The United States will continue to place a high priority on the provision of international technical assistance through our missions abroad and will continue to improve the coordination of these programs.

The United States will leverage all possible areas of cooperation, including legal instruments such as the UN Convention against Transnational Organized Crime (the Palermo Convention), the UN Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances, and the protocols to which the United States is a party, to obtain the assistance of international partners and to raise international criminal justice, border security, and law enforcement standards and norms. The United States will strengthen its engagement with the United Nations in this regard and leverage the growing role of regional and other multilateral institutions that have risen in significance and influence over the past decade. Additionally, the United States will continue to pursue cooperation with other countries and with partners such as the European Union, the G-8, the G-20, and new inter-regional platforms across the Pacific and Atlantic in developing leading-edge initiatives and political commitments to combat TOC.

The United States also will seek to develop informal partnerships with states that share U.S. goals to prevent TOC networks from abusing the benefits of globalization. By promoting flexible networks of law
enforcement and diplomatic partners, the United States can leverage the expertise and infrastructure of committed governments and respond more quickly to changing dynamics in transnational criminal threats. The United States convened a meeting of 25 countries and jurisdictions across the Pacific in April 2009 to consider common approaches and strengthen cooperation against transnational criminal networks that span East Asia, the Pacific, and Latin America. The United States hosted a similar event in May 2011 with the European Union to generate enhanced partnerships against trans-Atlantic criminal networks operating across Latin America, West Africa, and Europe. By building cooperative platforms and networks incrementally, the United States will generate greater collective action, joint cases, and common strategic approaches with our international partners to combat transnational criminal threats.

**Actions**

A. Raise international awareness of TOC and build multilateral cooperation against it.

B. Partner with countries able to contribute key law enforcement resources, other donors, and the United Nations to launch a new International Police Peacekeeping Operations Support Program to enhance policing and law enforcement capacity in ungoverned spaces.

C. Leverage assets to enhance foreign capabilities, including counterterrorism capacity building, foreign law enforcement cooperation, military cooperation, and the strengthening of justice and interior ministries.

D. Implement a public diplomacy strategy to reduce the demand for illicit goods and services that fuels TOC.

E. Implement the Central American Citizen Security Partnership to strengthen courts, civil society groups and institutions that uphold the rule of law in the region.

F. Implement the State Department’s West Africa Citizen Security Initiative to combat transnational criminal threats in the region.

G. Initiate new dialogue in multilateral fora to combat corruption and illicit trade, to include, as part of the Administration’s intellectual property enforcement strategy, stemming the flow of dangerous counterfeit products.

H. Build partnerships with other donors, private sector experts, nongovernmental organizations, civil society groups, the media, and academia that focus on supporting political will for criminal justice reform.

I. Increase international scientific research, data collection, and analysis to assess the scope and impact of TOC and the most effective means to combat it.

J. Institutionalize the U.S.-UK Organized Crime Contact Group to deepen bilateral cooperation and galvanize multilateral collaboration against TOC.


L. Expand cooperation with the United Nations to promote implementation of the United Nations Convention against Transnational Organized Crime, including through the development of an appropriate review mechanism.

* 27 *
M. Strengthen capacities for program management, internal controls, and contract administration to prevent the diversion or improper use of foreign assistance in countries threatened by TOC-related corruption.

N. Increase collaboration with international partners to improve their capacity to support immigration, customs, transportation, and critical infrastructure screening requirements and to harmonize their standards for screening and identification.

**Combating Transnational Crime: The Multilateral Framework**

Five major international agreements underpin and provide near global scope to our efforts to combat TOC and corruption: the United Nations Convention against Transnational Organized Crime (UNTOC), its three supplementary protocols against trafficking in persons, migrant smuggling, and illicit trafficking in firearms, and the United Nations Convention against Corruption (UNCAC). The United States strongly supports the framework provided by these instruments, especially with regard to prosecuting and investigating transnational crime and corruption engaging in mutual legal assistance and supplementing bilateral extradition treaties. These agreements set the point of departure for many of our bilateral law enforcement partnerships around the globe and help bring the international community into agreement with U.S. standards. The key challenge remaining is to promote wider implementation of the conventions through support for capacity building and by otherwise encouraging international partners to dedicate the necessary political capital and resources toward realizing the potential of these groundbreaking instruments.
Latin American Criminal Organizations Threaten United States National Security
Luz Nagle

Transnational organized crime from Latin America presents potent threats to United States national security and United States interests in the Americas. Organized crime groups are present throughout Latin America, with some of the most dangerous groups emanating from key U.S. allies Colombia, El Salvador, and Mexico. Latin America’s criminal organizations are both home-grown and international transplants from Asia, Europe, and Eastern Europe. Many have close ties to terrorist organizations operating in the region, such as Hamas and Hezbollah, and pseudo-revolutionary organizations that linger in the region such as the FARC and ELN in Colombia, the Zapatistas in Mexico, the Sandanistas in Nicaragua, and Sendero Luminoso in Peru.

The national security threats from organized crime include narcotics production and drug trafficking, human trafficking, money laundering, weapons smuggling, and document forgery. Organized crime is also involved in illegal logging and mining, and cattle rustling—activities that bring pressure on Latin American states whose formal economies are susceptible to the impact of black market trade. Latin American states that are engaged in delicate trade arrangements with the United States are particularly threatened.

Organized crime also destabilizes judicial institutions, which weakens the governability of states in the region and has a chilling effect on the protection and enforcement of commercial transactions and foreign investment.

Among the most debilitating elements of organized crime is the spread of corruption into local, state and national government institutions. Corruption crosses all
political parties and has spread into the United States, as evidenced by several incidents documented in early 2013 by the Government Accounting Office involving corruption of U.S. border patrol agents along the U.S./Mexico border.\(^1\)

The Corruption Perceptions Index, maintained by Transparency International, underscores the extent to which corruption threatens the rule of law in Latin America. In 2012, of 176 nations represented in the Index, only Chile and Uruguay fall within the top twenty countries perceived to be the least corrupt in the world. Costa Rica and Cuba ranked at 48 and 58, respectively. Of the remaining Latin American nations, nearly all rank in the lower half, with Venezuela occupying the ignominious rank of being the 165th most corrupt country in the world (tied with Haiti).

The US intelligence community also sees a deepening relationship between terrorism and organized crime, particularly in states hostile to the United States and having populist governments, namely Argentina, Ecuador, Nicaragua, and Venezuela.

Three regions in Latin America pose a particularly significant threat to United States interests due to organized crime, terrorists, and first generation gang activities: the northern triangle countries of Honduras, El Salvador and Guatemala, the tri-border area of Brazil, Paraguay and Argentina known as the Iguaçu triangle, and the Venezuelan island of Santa Margarita.

In addition to what one may think of as “traditional” criminal organizations, new organized criminal groups have formed in the region, namely derivatives of the mara salvatrucha gangs present throughout Central America and BACRIMs in Colombia.

\(^1\)“According to the GAO’s findings, since 2005, 2,170 agents have been arrested for non-corruption charges such as domestic violence and driving while intoxicated. However, 144 were arrested or indicted for direct corruption-related activities such as drug and human smuggling. By Oct. 2012, 125 of these agents had been convicted.” See Joseph Kolb, Study finds corruption on rise among border agents, rep says security ‘at risk’, FoxNews, Jan. 15, 2013.
BACRIM groups compete for hegemony in the poor urban environment in order to carry out criminal enterprises. These groups are a "hybrid" of three illegal armed groups: criminal gangs, paramilitary forces, and narcotraffickers, and comprised of former paramilitary combatants and sundry criminal actors. They have been referred to by the Colombia National Police commander as Colombia’s greatest current threat to national security, composed primarily of demilitarized paramilitary combatants, that have emerged as the serious threat to Colombian national security and increasingly poses a threat to US interests in the region.

The following is brief summary of activities of criminal organizations and terrorist groups in Latin America that pose a direct threat to the United States in the following ways.

The Zetas in Mexico are now entrenched in drug trafficking into the United States. They have terrorized government officials and their violent reach extends well north of the U.S./Mexico border. The United States continues to combat criminal organizations like the Zetas and other Mexican drug cartels, using precious financial resources year after year that could be put to more productive use elsewhere.

The tropical resort island of Isla de Margarita just off the coast of Venezuela was once famous as a world-class windsurfing destination. In the last decade under the rule of President Hugo Chavez, it became a world-class destination for money laundering and

---

a safe haven for Islamist terrorist organizations Hezbollah. In fact, the United States Treasury Department blacklisted the number 2 Venezuelan diplomat in Syria in 2008 “for fundraising and logistical support to Hezbollah,” and running a network that “raises and launders money and recruits and trains operatives to expand Hezbollah’s influence in Venezuela and throughout Latin America.” The terrorist organization, Hamas, is also involved in nefarious activities in Isla de Margarita and both organizations used the island as a staging base to infiltrate its operatives in the United States and elsewhere throughout Latin America.

Hezbollah is also present in the tri-border region of Argentina, Brazil, and Paraguay. This essentially lawless region has been an ideal safe haven for terrorists for decades and is often referred to as the United Nations of Crime. Terrorist cells are believed to have staged out of the tri-border to launch attacks on the Israeli embassy and a Jewish community center in Buenos Aires in the early 1990s. In Paraguay, the Hezbollah is known to be heavily involved in a four-story shopping center, Galeria Page, in Ciudad del Este, Paraguay. The US Treasury Department has long considered the Galeria Page the center of money laundering operations and counterfeiting of US dollars operations in Paraguay.

---


Finally, continuing poverty and disenfranchisement of large segments of Latin American society create fertile ground for dissident development and recruitment of foot soldiers by terrorist organizations and organized crime. Unless the regions inhabitants become fully invested stakeholders in the civil society, the region remain uncertain and poses a simmering caldron threatening United States national security and interests in the region.
TO WHAT EXTENT DO GLOBAL TERRORISM AND ORGANISED CRIMINALITY CONVERGE?: GENERAL PARAMETERS AND CRITICAL SCENARIOS

To what extent do global terrorism and organised criminality converge? General parameters and critical scenarios Despite their differences in terms of motivations and methods, historical examples indicate that terrorism and organized criminality can converge in several ways. Indeed, some analysts think that both threats can no longer be studied in isolation. This report explores the hypothesis of a crime-terror nexus for the special case of global (jihadi) terrorism. Three types of convergence are examined: involvement in criminal activities by terrorists, transformation of terrorists groups into hybrid or purely criminal organizations and cooperation between organized criminal organizations and terrorist groups. Finally, the study ends with a section dedicated to the cases of Af-Pak, Iraq and Western Sahel, presented as examples of privileged scenarios for interaction between global terrorism and organized crime.

global terrorism, organized crime, convergence, terrorism-organized crime nexus, drug traffic, kidnappings, criminality, failed states.
TO WHAT EXTENT DO GLOBAL TERRORISM AND ORGANISED CRIMINALITY CONVERGE?: GENERAL PARAMETERS AND CRITICAL SCENARIOS

1. Introduction

Two lines converge when their courses interchange or they meet at one point. This may also occur with the paths that terror and other criminal activities plot out. Without establishing a wholly new subject, the study of the actual— or potential—convergence between terrorist activity and organised crime has been gaining interest in recent times. As Walter Laqueur has stated—a renowned historian to whom we owe some of the first and the most significant academic studies on political violence: while up to fifteen years ago, all concepts postulated a sharp division between terrorism and organised crime, with the passing of time the border that separates them has become increasingly blurred. In recent years, the change in perspective has gone so far that some experts suggest the necessity of doing away with this distinction, at least for certain cases of a clear symbiosis between one phenomenon and the other. Some of the information and focuses provided by the mass media tend to reinforce this new approach, whether by means of news reports that assure us the involvement of terrorist groups and organisations in typical activities of common or organised crime, or by attributing characteristics of an unquestionably Mafioso nature to others.

In short, the opinion has started to spread that the convergence between terrorism and organised crime could come to be a growing trend within the geo-political framework inaugurated at the end of the XX century. There are various factors for change that would push us toward that direction. On the one hand, the end of the Cold War and the proliferation of anti-terrorist laws have drastically reduced the willingness of States to sponsor terrorist groups or organisations, inducing them to use other means of financing (including those relating to conducting illegal activities).

2 Hereinafter the terms “organised crime”, “organised criminality” and “organised delinquency” will be taken to be synonymous expressions.
In a complementary sense, the transition towards a globalised economy and world and the consequent emergence of a transnational form of organised criminality has considerably increased the possibilities for terrorists to become involved in illegal businesses\(^4\). These arguments explain that the connection between international terrorism and transnational organised crime is a threat that is contemplated in most of the recent strategic documents.

Basing ourselves on data, evidence and research that has been available to date, this paper initially examines to what extent the convergence with organised crime is rather more than a hypothesis for the case of global terrorism, and with which expressions and modalities that phenomenon can be demonstrated.

2. Some preliminary conceptual clarifications

Conventionally speaking, the terms “terrorism” and “organised criminality” are the name given to activities that are partly similar and partly different. Leaving the absolutely exceptional examples of individual terrorism to one side, amongst the features that are common to organised crime and terrorism we can highlight their relationship with illegal and “organised” activities, those that result from a concerted, coordinated and recidivist form of action carried out by a set of individuals or a human group with a minimal degree of structure. Very often, furthermore, factors appear that are associated with one essential component of the terrorism, such as practising violence. Such similarities go to show why some penal codes define terrorism as a sub-type of organised criminality, which would be distinguished from the general type of it in two essential aspects: a more direct and systematic relationship with the continuous practice of violent activities or armed actions (used to make population, or one sector of the population fearful) and the association of such practices with a political purpose. Given the significant differences that these two attributes usually impose on the functioning of terrorist organisations, one alternative focus prefers to take its exclusive reference point for the concept of “organised criminality” to be those criminal phenomena that, in addition to being attributed to collective or organised individuals, have the unique or main objective of obtaining and accumulating economic or material benefits\(^5\). Starting from this second focal point, which we will make use of from now on, organised criminality carries on two types of complementary illegal activities. The first ones are those that seek economic gains for the particular criminal organisations and that take up most of their time. This includes a wide range of criminal options:


illegal trade of all types, extortionate practices, robberies, attacks and (paid) killings, labour and sexual exploitation, frauds and swindles, unlawful financial services, etc. Secondly, such lucrative activities are usually complemented by some acts that are not always remunerated, which perform significant facilitating or protective functions: essentially corruption, violence and money laundering.

In turn, the term “terrorism” tends to designate a particular type of violent activity: although, by extension, it is frequently used to refer to those individuals, groups and organisations that systematically practice it. Above all, what distinguishes acts of terrorism from other types of violent action is their capacity to provoke an intense social or psychological impact (anxiety or fear) that is disproportionate with respect to the physical damage caused to the people or objects chosen as targets of the aggression. As has already been indicated, most of the groups and organisations that resort to terrorism do so being encouraged by the argument of conditioning the attitudes and the form of behaviour of governments or of political communities. For this reason, and in accordance with numerous institutional and academic definitions, all of our references to terrorist activities and entities will correspond to cases that include an exclusively political motivation or that ties together politics and religion.

During recent decades, organised criminality has undergone an intense process of trans-nationalisation, which is the result of three trends that have been developed: a substantial increase in cooperation between criminal groups and organisations with a different location; the emergence of various unlawful global markets, with some business stages distributed in different regions of the world (the best example is provided by the worldwide trade in drugs); and the appearance of criminal organisations with an active presence or implementation on an international scale.

Albeit with less generality than that corresponding to the transnational development of organised criminality, the evolution of terrorism in the XX century has also created its particular patterns of trans-nationalisation. The accumulated evidence indicates that these patterns have thrown up quite a few connections with the world of organised crime. Nevertheless, this analysis will only be concerned with the criminal

---


7 This definition is inspired by the parameters set out by diverse studies such as: REINARES, Fernando, Terrorismo y antiterrorismo [Terrorism and anti-terrorism], Barcelona, Paidós, 1998; DE LA CORTE, Luis, La lógica del terrorismo ["The logic of terrorism"], Madrid, Alianza, 2006; Transnational Terrorism, Security, and the Rule of Law, Defining Terrorism, Brussels, 2008. Available at: http://www.transnationalterrorism.eu/tekst/publications/WP%20Del%2004.pdf

8 A similar option when it comes to deal with the subject of this research can be found at BOVENKERK, Frank y CHAKRA, Bashir Abo, "Terrorism and organized crime", UNODC Forum on Crime and Society, 2004, vol. 4, nº 1 and 2, pp. 3-16; WILLKINSON, Paul. Political Terrorism, Nueva York, Willey, 1974.

nexus that entail the latest and the most extreme modality of transnational terrorism: that which some experts have agreed to call “global terrorism”. In general terms, this concept can be applied to any form of terrorism which, taking advantage of the conditions of economic, political, informative and cultural interconnection that characterise the globalised world of the XXI century, has the determination and the capacity necessary to produce repercussions (psychological, social, informative and political) of a worldwide extent. In empirical terms, the emergence of this class of terrorism appears to be closely linked to the formation of the Al Qaida organisation and of the diffusion and complex mesh of organisations, groups and individuals that have acted under its influence: whether as a consequence of the direct communication and cooperation with its top leaders or due to mere ideological following.

3. Modalities of convergence and examples associated with global terrorism

Various interpretations have been put on the consideration of the convergence between terrorism and organised crime, or between organised crime and terrorism. For a long period of time, most of the studies of terrorism that deal with the subject, in largely abstract terms, made use of one of the two opposing hypotheses. In the first one, the convergence between terrorism and organised criminality would be little less than a “contra natura” option. According to the second one, on the other hand, this deals with a spontaneous, quasi-natural tendency. Those in favour of the first position usually seek to justify their theoretical justification by detailing the benefits that may derive from the convergence between one activity and the other, and the similarities between both of them. In contrast, the critics of the convergence hypothesis underline the prejudices that this trend may represent for those involved in it, as well as the differences (in objectives and means) that distinguish the terrorists from organised criminals. Nevertheless, the accumulated evidence over several decades of research into terrorist phenomena go beyond the specific type that concern us (global terrorism), showing two main conclusions.

Firstly, the convergence between terrorism and organised criminality is neither natural nor against nature. The hypothesis that considers this has found empirical confirmation in more than a few cases. Hence, convergence is an unquestionable possibility and a comparable pattern. However, the opposing examples are more numerous and


significant, making it hard to maintain the idea of a generalised trend towards converging. On the other hand, and in the form of a second conclusion, the positive cases of convergence do not all follow the same pattern, but rather they make it possible to identify various alternative modalities.

The variability of the terrorist-criminal convergence cases can be summarised by means of a taxonomic composition made up of three differentiated categories.

3.1 Confluence: involvement in other criminal activities

This could also be called "convergence by appropriation of methods" and it deals with the most basic form of this. It occurs when terrorist groups or organisations are involved in activities that are typical to organised criminality. We are essentially referring to criminal actions of a different nature, chosen so as to meet logistical or financing needs. We set out an incomplete list below, illustrated with a specific example that involves groups or organisations that form part of the global terrorist (jihadist) sphere:

1. Drug-trafficking. This has been developed in two ways: on a large scale, as is proven by the significant involvement in the trafficking of poppies by the Taliban and other jihadist groups with a presence in Afghanistan and Pakistan (the Haqqani network is highlighted) or Central Asia (with the preponderance of the UIM, Uzbekistan Islamic Movement); on a small scale, as happens in the case of the small amounts of hashish trafficked by Jamal Ahmadani, one of the

---


perpetrators of the attacks in Madrid on March 11, 2004.\textsuperscript{16} In all of the cases, these forms of participation in the drug business similarly require a complementary form of convergence: assistance from professional drug traffickers. We will look at this issue later on.

2. Other illegal trade. According to some information, at the start of the last decade Al Qaeda may have made use of the black market in gold and precious stones so as to obtain funds, conceal part of its money, launder profits from illegal sources and convert its funds in cash into objects that keep their value and were easily transportable. Although the P	extsuperscript{II}-S Commission report refuted that evidence had been found in this respect, some experts still give credibility to the accusation that alleges that Al Qaida was involved in operations of buying and selling diamonds\textsuperscript{17}. Another significant product that is trafficked with the help of jihadist groups is tobacco. The involvement of AQIM in smuggling cigarettes is relatively well-known (we will come back to this in another section). Nonetheless, Afghan and Pakistani jihadists also seem to have been making profits from this illegal activity\textsuperscript{18}. The trade in human beings has involved, amongst others, the Algerian GIA, as well as Yemaa Islamiyya, the most powerful terrorist structure in south-east Asia that has maintained links with Al Qaida, whose main base is in Indonesia\textsuperscript{19}.

3. Theft. Once more, Yemaa Islamiyya is a notable example, amongst many others. In fact, this organisation used robberies from several Banks as a means of obtaining the money necessary to fund its most deadly terrorist attack, a multiple attack perpetrated on the island of Bali on October 12, 2002. The final count was over two hundred victims killed\textsuperscript{20}. The Pakistani Taliban have also taken part is several robberies from bank offices. In turn, the jihadist networks established in Spain from the end of the 90's made use of the theft of credit card as one of their means of financing\textsuperscript{21}. This particular criminal pattern, along

\textsuperscript{16} National Court. Criminal Division, Second Section, Ruling no. 65/2007. Second Section Summary proceeding number 20/04 of the Central Magistrates Court no. 6, Division Roll no. 5/05.


\textsuperscript{21} DE LA CORTE, Luis and JORDÁN, Javier. La yihad terrorista [The terrorist jihad], Madrid:
with the theft (and subsequent sale) of other small items (mobile phones, GPS devices, watches) has been identified in the jihadist cells established in other European countries, including Switzerland, Italy and France.\footnote{\textit{Del CID GÓMEZ, Juan Miguel. “A Financial Profile of the Terrorism of Al Qaeda and its Affiliates”. Perspectives on Terrorism, vol.4, no 4. 2010.}}

4. Forging of documents. Given that this activity covers one of the chief logistical needs of terrorist groups and organisations, it is not surprising that they work together with individuals from the criminal world who have previous experience as forgers. This is what happened with Ahmed Ressam, an individual associated with the Algerian SGPC, who was arrested in Washington in 1999 when he was trying to bring explosives into the United States so as to carry out an attack at Los Angeles international airport. This individual whose intentions fell within the scope of an ambitious terrorist plan developed by Al Qaida (the Millennium Plot) entered the United States from Canada using false documentation that he had obtained himself. In reality, Ressam had spent some years in Canada, obtaining money from theft and forging documents\footnote{\textit{JORDÁN, Javier. “Un estudio preliminar sobre las tendencias del terrorismo yihadista en Europa” [A preliminary study on the trends of jihadist terrorism in Europe]. Essays from the CESEDEN, 122, Ministry of Defence, Madrid, 2008, pp. 205-235: DE LA CORTE, Luis and GIMÉNEZ-SALINAS, Andrea. “Yihadismo en la Europa comunitaria: evolución y perspectivas de futuro” [Jihadism in the European community: evolution and future prospects], in Athena Assessment. 4. 2008.}}. This is the same profile as a certain number of jihadists arrested in Spain during the decade of the 2000’s.\footnote{\textit{KREBS, Brian. “Three Worked the Web to Help Terrorists”. The Washington Post, 6/7/2007. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070502451.html}} A significant operation carried out in the United Kingdom showed that three members of a terrorist cell were planning to carry out attacks in the United States, Europe and the Middle East, and that they used various stolen credit cards so as to buy different articles that they wanted to send to jihadists in Iraq (some of these articles were GPS devices, night vision glasses, telephones or knives)\footnote{\textit{U.S. Department of the Treasury. Remarks of Under Secretary David Cohen at Chatham house on “Kidnapping for Ransom: The Growing Terrorist Financing Challenge. October, 2012.}}.

5. Kidnappings. Leaving aside the examples of the illegal capture and holding of people with the exclusive aim of forcing political concessions and obtaining publicity, kidnappings for extortion constitute a recurring mode of financing in the general history of terrorism, and also in that of some of the regional or local individuals associated with global terrorism\footnote{\textit{SAGEMAN, Marc. Understanding Terror Networks, Philadelphia: University of Pennsylvania Press. 2004. p. 100.}}. The AQIM joining in with the
kidnapping business at the end of the last decade (an issue that we shall return to later on) is the experience that is most well-known and perhaps the most worrying one: but by no means is it unique. Going back further than that, but in no way less interesting, is the case of Abu Sayaff, a Philippine organisation close to Al Qaida, that became involved in recent years in the undertaking of kidnappings and the subsequent ransom demands (in combination with some drug-trafficking operations)\textsuperscript{27}. Other groups that have used kidnapping to obtain ransoms are the jihadist insurgents of Pakistan and Iraq.

6. Extortion for protection. The use of intimidation and threats, as a means of collecting specific or regular sums of money, is an old criminal method. For example, aggression and threats for the purposes of extorting money from traders and professionals of different levels has become a generalised practice amongst the terrorist groups established in different provinces and regions of Pakistan: from the tribal regions, Afghanistan, to the more developed provinces of the Punjab and Sindh. The usual victims of these acts of extortion are traders and professionals of different types. This practice is sometimes based upon the kidnapping of the particular individuals subject to extortion or their family members. The terrorist groups involved include Jihadist elements such as the TTP (Tehrik-e-Taliban Pakistan, or the Pakistani Taliban) and the Haqqani Network\textsuperscript{28}. Specifically, some information indicates that radical Pakistani groups have obtained funds in Spain by carrying out extortion on compatriots who were living in our country. In some cases, these forms of extortion were in the form of express kidnappings\textsuperscript{29}.

7. Creation of front or screen companies. The concealment of money from illegal activities and mixing this in with legal money, are basic requirements for the accumulation of profits by criminal organisations. The creation of companies orientated towards this purpose is a traditional resource of organised criminality, though it has also been used to hide the movement of funds used to pay for terrorist actions. A detailed sample was obtained from the operation targeted against the first cell established by Al Qaida members in Spanish territory and that led to it being partially dismantled (Operation Date, in November 2001). As that investigation showed, the financing head of that cell between 1996 and 2001 was Ghaleb Kalaje Zouaydi, and he used diverse legal companies (including a real estate agency set up in Spain), to divert a minimum of 670,000 Euros, with the aim of financing terrorist activities (this particular cell also

---


\textsuperscript{29} DEL CID GÓMEZ, Juan Miguel, op.cit.
obtained money from forging documents and credit cards).\(^{30}\)

8. Others. Together with the crimes described, there is evidence that proves participation in some cyber-crime operations. For example, while the same jihadists arrested in the United Kingdom in 2007 were carrying on the operation mentioned above, they made use of betting web sites to launder party of the money that had been extracted from stolen credit cards. These same individuals used those particular cards, and several sets of numbers stolen from bank accounts, in order to buy internet services and to create virtual networks that could be used by jihadists all over the world as a means of exchanging information, recruiting militants and planning attacks.\(^{31}\)

3.2 Hybrid blending or transformation: from terrorism to organised crime

When their involvement in illegal businesses and operations becomes something that recurs or is systematic, and numerous lines of revenue are produced, the possibility arises that the terrorists can raise the value attributed to these illegal practices, to the point of taking on the economic motivation that is characteristic of organised criminality. This change can be substantiated on two levels: the first one entails the group or organisation evolving towards a hybrid structure, halfway between terrorism and organised criminality. The second one, on the other hand, entails the transforming of a terrorist network into a mere criminal organisation, preferably one that is geared towards the accumulation of economic profits. The pattern followed in this second option usually involves the original ideological facade being maintained, which makes it hard to distinguish these cases from the previous ones.

Amongst those people involved who have maintained some link with the worldwide jihadist movement, there are few that have followed this path; and yet we are not short of some illustrative examples, whose names have already appeared in these pages. There is no doubt that Abu Sayyaf is one of these. In spite of having come from the most radical wing of a separatist Muslim movement, following the death of its first leader Abdurajak Janjalani, in 1998, this Philippine organisation initiated a new phase that was focused on kidnapping and collecting ransoms, as well as becoming involved in some drug trafficking and money forging operations.\(^{32}\). This change would lead to most of the analysts making reference to the transformation of Abu Sayyaf into a


\(^{31}\) KREBS, Brian, op. cit.

simple criminal gang. A similar judgment was applied to the UIM (Uzbekistan Islamic Movement). This is an organisation that came to control 70% of the routes that Afghan opium and heroin passed through during the 2000’s, and this was later sent on to different Central Asian countries. Nevertheless, inasmuch as none of these groups has publicly renounced neither violence, its thinking, it political goals or religious ones, it seems prudent to consider that are both still examples of hybrid blending between terrorism and organised crime. This is not necessarily incompatible with economic motivations predominating amongst the militia, to the detriment of policies.

3.3 Cooperation with criminal gangs and organisations

There are two forms and different levels in the way that terrorist groups and gangs and organised crime work together. One takes place when a criminal gang or organisation decides to provide support to a terrorist structure, due to reasons of ideological or religious affinity. This is an option that is rather less than abstract, with just a few empirical illustrations. As regards this subject, the closest possible case is perhaps that of the D-Company, an Indian criminal organisation of Muslim militants whose leader, Dawood Ibrahim, was the top criminal boss of Bombay for many years. He was highly involved in the trafficking of drugs, weapons and human beings, and in activities of extortion and money laundering. A wave of street attacks against the Islamic population, unleashed in India between 1992 and 1993, fostered the radicalisation of Ibrahim and this followers, until it brought about close cooperation between various jihadist groups in the region and the Pakistani terrorist organisation Lashkar-e-Tayyiba, a natural ally of Al Qaida. This cooperation too the form of joint participation in various campaigns of attacks on Indian soil that led to hundreds of deaths.

The second form of collaboration stems from purely practical interests and this entails a material or economic transaction exchange. Buying weapons, explosives or false documentation from criminal gangs is a resource that terrorists can make use of when they are short of the capacities or opportunities necessary to obtain these products by their own means. Thus, different reports substantiate that various militants of Al Qaida itself maintained contacts with Russian and Eastern European criminal organisations, with the aim of buying nuclear, chemical and biological material, although it would seem that the gangsters ended up cheating the terrorists in the transactions they carried out. Here it is also worth mentioning the jihadist networks responsible


36 WANNENBURG, Gail, op. cit.
for the attacks perpetrated in Madrid on March 11, 2004. In that case, the terrorists used explosives that they had obtained in exchange for a certain quantity of hashish. A different example is the role played by the cells that Al Qaida managed to set up in the Balkan region in the nineties, as a result of the logistics support provided by Albanian criminal organisations which, in turn, were collaborating with the Kosovo Liberation Army.

Leaving aside some scenarios that are especially favourable to contact between terrorists and criminal organisations, which we will deal with later on, collaboration for pragmatic reasons is not particularly frequent either. In most of the cases that are known, these exchanges are limited, sporadic or particular to that instance, and these are determined by a need that has to be resolved urgently or due to taking advantage of a transaction opportunity that is particularly attractive. All in all, there are times in which the initial collaboration may give rise to the creation of associations that last longer and are more wide-ranging.

4. Critical scenarios for convergence: the cases of Af-Pak, Iraq AND Sahel

In the same way as with any other criminal practice, terrorism and organised criminality are dependent activities in their context. Not all settings and circumstances make them possible or foster them to the same extent. Moreover, each setting and time may modulate their development, generating specific and varied patterns and expressions. The same can be asserted about the convergence between both threats. Probabilities in this regard also change, depending on the circumstances. Not all circumstances are equally favourable towards terrorism and organise crime, while some especially facilitate it.

One type of facilitating scenario relates to environments that are typically crime producing such as jails, deprived neighbourhoods and areas of large cities and towns or enclaves that touch upon several borders. There are others, however, that span across wide geographical areas: from large portions include within one country to entire nations or multinational regions. It has been precisely in this second type of spaces where the affinities between global terrorism and organised criminality have progressed to the highest level. This connection is demonstrated, Af-Pak, Iraq and the Western Sahara, three convergence scenarios whose examples we shall examine below.

4.1 Main features of the three scenarios

In spite of being located in different and distant geographical settings, marked by

---

their own particular features, it is clear that the scenarios selected share some characteristics and problems, and it does not seem to be accidental that these are repeated. As a minimum, it is worth listing the following ones:

1. Multi-frontier and porous border.
2. State fragility or weakness.
3. Ethnical and tribal heterogeneity.
4. Lack of institutional legitimacy.
5. A lot of corruption
6. Armed conflicts.
7. Underdevelopment or critical economic situations.

These characteristics simultaneously contribute towards fostering the two types of threats that concern us here, terrorism and organised crime. In doing so they extend the motivations that inspire them, both the capacities and opportunities that make them possible. The problems of legitimacy attributed to the established political order, ethnic tribal tensions and the catalyst for armed conflicts (especially those that stem from foreign military intervention or involve the presence of foreign troops, supporting some of the bands that are at loggerheads), extending the reasons for practising terrorism. The problems of food and provisioning deriving from underdevelopment, from poor government and from the armed conflicts, along with the economic crises and limitations in the same way, engender the appearance of illegal markets that are exposed to the risk of falling under the control of criminal gangs and organisations. In turn, the options for developing these illegal markets are multiplied thanks to corruption, to the existence of porous or badly monitored borders and the relationships of trust based upon ethnic or tribal sentiments and commitments of solidarity. Lastly, the fragility or institutional weakness increases the opportunities from crime and terrorism, by limiting or drastically cutting back the repressive capacities of the State. The most extreme examples in this respect can be seen in those scenarios where the inability of the institutions to operate extends so far that the State loses its capacity to perform its basic functions. In this way, it enables terrorists and criminals to act and interact with complete impunity (which we have elsewhere referred to as the “gas in sovereignty”).

Each and every one of these ways of facilitating terrorism and organise crime, taken in context, have been observed in Af-Pak, Iraq and the Sahara, with the twofold consequence of multiplying the possibilities of convergence between one phenomenon and the other. At the same time, this reduces some of the main costs that, as a general rule, are inherent to such a form of interaction.
4.2 Predominant criminal activities

4.2.1 Drug trafficking

Another element shared by the three convergence scenarios that are examined here is the involvement of the terrorist individuals in several of the typical activities of organised crime included in the general list that we set out in an earlier section.

Following the same order used here, the first category of notable criminal activities is drug trafficking. The merchandise that is most commonly trafficked in Af-Pak is opiates. This is not coincidental, given that for some decades Afghanistan has figured as the leading opium-producing country, with a great advantage over any other one (about 90%). We cannot say that it is a coincidence either that for years most of the opium from Afghanistan has been grown in the south-western province of Helmand, the strategic centre for the Taliban and other jihadist groups of the Pashtu ethnic group. In more general terms, the cultivation of opium in a minimum of 34 Afghan provinces and the exporting of this to the rest of the world, would have been impossible if they had not had the backing from and participation of the insurgent and terrorist organisations and gangs of Afghanistan, Pakistan and Central Asia that we have already referred to before. Over the course of the decade of the 2000s, this amalgam of local insurgent activists, associated with global jihadism, have taken part in nearly all of the operations that fall within the drug business cycle. They generally act as facilitators and protectors: from the growing of the opium, moving on through the processing of it as it is transformed into heroin, the storage and transporting of it, or its ultimate exportation and sale. By way of example and starting from the basis of the estimates made for the period 2005-2008, the support of the Afghan Taliban for these activities could have brought them a minimum income of greater than 125 million dollars per year.38

In recent years, the news has emerged that relates the AQIM to the cocaine that comes from the American continent that is moved into Europe, first having passed through the Western Sahara. In spite of the data obtained from an operation conducted by the leading United States anti-drug agency (the DEA) in that region, the existence of ties of cooperation between AQIM and the Colombian FARC has emerged, it has not been possible to date to demonstrate with certainty that there is indeed a relationship of this type. All in all, most experts assume that the jihadists of the Sahara have for some time been applying charges to the cocaine traffickers who cross the territories that are under their control, in return for allowing the drug to be moved and protecting the convoys in which they transport it.39 This particular measure seems to


be applied to the cargos of hashish that come from north Africa⁴⁰.

4.2.2 Kidnappings

The other criminal measure with significant jihadist involvement in the scenarios examined was to commit kidnappings for extortion, especially in the Sahara and in Iraq. This topic is relevant, both due to the frequency with which it is practised and because of the income it provides. Although there had been precedents, which occurred in the Sahara desert in the final years of the last century, the SGPC terrorists started up this activity in February 2003, kidnapping 32 tourists in a southerly part of Algeria. 17 of those tourists were released at no cost, while the other 15 were moved to Mali, and they were set free 6 months later. In 2008, and after having taken the name of AQIM, the organisation of Algerian origin set underway an intense and prolonged campaign of kidnappings. To April 2012, these actions took the form of the kidnapping of 42 foreigners captured in different countries (Algeria, Tunisia, Mauritania, Niger and Mali), who were subsequently moved to the north of the latter country. In recent years, 24 hostages were released and a further five were killed, some at the time they were captured and others during their captivity. There were still seven hostages in the hands of AQIM at the start of 2013. On January 16, 2013, a spin-off from AQIM led by Belmokhtar conducted a hostage-taking operation at a gas plant located in the east of Algeria, close to the border with Libya, holding 40 foreign workers and 150 Algerians. The crisis was resolved several days later, thanks to an intervention by the Algerian army, which resulted in the dramatic count of 23 hostages and 32 terrorists dead. Whilst in the same way as in other earlier operations, the kidnappers presented the operation as an act of political pressure; it is very likely that their true intention was to escape with the hostages so they could then be released in exchange or a sizeable ransom. In practice, it seems that none of the foreign hostages captured by AQIM in recent years have been released without substantial payments having been made. The fact that some States refused to pay the kidnappers, and due to some frustrated rescue operations, several hostages died. While it is hard to ascertain the income that that has actually been obtained from the kidnappings carried out in the Sahara, some estimates indicate that the cost of each hostage must have reached estimated figures of between a


Hocine, Boukara; Messaoud, Fenouche; Lotfi, Touati; and Karima, Benhadj. "El terrorismo y sus enlaces con el tráfico de droga en África subsahariana" ["Terrorism and its connections with drug-trafficking in sub-Saharan Africa"]. In SPANISH INSTITUTE OF STRATEGIC STUDIES (SISS) and MILITARY INSTITUTE OF DOCUMENTATION, EVALUATION AND PROSPECTS OF ALGERIA (MIDEP), "Terrorismo y tráfico de drogas en África subsahariana" ["Terrorism and drugs in sub-Saharan Africa"]. Work document of the Spanish Institute of Strategic Studies. 13/3/2013. Available at: http://www.ieee.es

million and a half and four million dollars. It has also been calculated that, since 2008, the jihadists and their collaborators have made the kidnappings profitable, with income that would range between 40 and 65 million dollars. Similarly, various payments received from kidnappings in the Sahara have been accompanied by the release of criminals and militants who had been held in prisons in Mali or Mauritania. The people released have included AQIM militants and those from one of their jihadist allies in the region such as the MOJWA (Movement for Oneness and Jihad in West Africa).

The data available about kidnappings in Iraq are no less significant. Facilitated by a tradition of kidnappings related to tribal disputes, business conflicts and forced marriages, after the fall of Saddam Hussein, this activity quickly became a kind of epidemic in which old and new criminal networks profusely participated, along with the insurgent factions. Very soon, the kidnappings came to represent 70% of registered crimes, with an average of two kidnappings per day. In 2004 alone, that proportion grew from two to a total of ten incidents per day. It has been estimated that in the time of greatest activity, there was an average of 6,000 kidnappings per year. Unlike what has happened in the Sahara, foreigners in Iraq only constituted one of many other targets for the kidnappers, and it has been the figure of Iraqis kidnapped that has overwhelmingly predominated. The national victims have included government officials, businessmen, bankers, university lecturers and scientists, women, teenagers and children. The average price of each ransom has been calculated at around 25,000 dollars per hostage. The coalition governments that succeeded Saddam Hussein in power have recognised, in their internal documents, that they have paid several million dollars with the aim of ransoming numerous of their citizens who had been kidnapped. One of the most reliable reports on the issue indicates that this business could have contributed between 100 and 150 million dollars per year, without counting the money obtained from foreign kidnappings. According to the same study, it also says that this figure may well have exceeded one hundred million dollars. Even when the kidnappings have been much less common, the ransom prices have been very much higher. On the other hand, the researchers state that it is not possible for them to specify what is the proportion in which the income from kidnappings has been distributed amongst the insurgent criminals. The charismatic and much-feared leader of AQI (Al Qaida in Iraq), Abu Musab al Zarqawi, launched a campaign involving the recorded decapitations of western foreigners that were subsequently distributed through the media. In this way kidnapping became a weapon of intimidation and political pressure. The first example of this became known on May 11, 2004. This was the day on which a video appeared on Internet that showed the decapitation of the American citizen Nicholas Berg, who his kidnappers accused of being involved with

the notorious Abu Graib prison. While other captured victims ended up in the same way, the jihadists gradually came round to the idea of kidnapping as a business, charging money to release hostages. However, it has not been possible to specify the gains obtained by this means to date.

4.2.3 Other significant criminal activities: extortion, further illegal trafficking, theft and swindles.

The jihadist factions established in Af-Pak, Iraq and the Western Sahara have limited themselves to other characteristics of organised criminality in addition to illegal trafficking and kidnappings. In the previous sections we have already mentioned the extortion practice carried out in Pakistan and Afghanistan by jihadist groups close to Al Qaida, imposed on various segments of the population and of the local businesses. Nonetheless, extortion has equally been used in Iraq and in northern Mali42. The reinforcing of this, from 2004, allowed for the Sunni insurgency to defeat the Coalition forces in the control of the motorways, which then translated into the imposing of transit costs. The victims of these ransom collections would include the foreign and national contractors that that had to carry out the reconstruction of the particular motorways as well as the drivers who transported all kinds of merchandise, whether legal (especially food, fuel and engineering material) or illegal (such as products stolen for smuggling). In these latter cases the extortion could be complemented by part of the confiscation of part of the material transported. Thus, in the time in which the air and railway services were not operating in most of the country, any lorry loaded with fuel that was travelling by motorway would be required to make an average payment of some 500 dollars. In turn, quite a lot of contractors and businessmen would get used to inflating their estimates so that these include the sums of money necessary in order to avoid attacks, kidnappings and other acts of sabotage by criminal and insurgent groups. Another significant target for extortion by the jihadist and lay insurgents were the Shia and Christian minorities that were established in regions under Sunni control. This was a practice that incidentally was reproduced by Shia militants in their areas of influence. Extortion in Iraq was particularly intense during the four years that followed the 2003 invasion. Thirdly, it has also been possible to contrast the fact that the establishing of a jihadist settlement in northern Mali in 2012 came in association with the application of extortionate practices on the local population. In addition to this there is the forced collection of taxes imposed on the staff of non-governmental organisations, and in these cases tolls of up to 50,000 francs were imposed on every vehicle that went into the area with the intention of giving out humanitarian aid43.

---


43 Reinares, Fernando. "Un condominio yihadista en el norte de Mali: ¿cómo ha surgido? ¿se consolidará? [A jihadist establishment in northern Mali: how has it come about? will it become con-
Another criminal activity of significance carried out by the jihadists involved in the scenarios that we have been analysing relates to various forms of illegal trade. Both the Afghan Taliban and the rest of the Af-Pak jihadists have complemented their income related to drug trafficking by means of their participation in operations of trafficking in chemical precursors for preparing drugs, cannabis, weapons, precious stones, tobacco and wood. These illegal forms of trade have also performed a significant role amongst the activities that have concerned the katibas or branches of AQIM that have put down roots in the western strip of the Sahara, here smuggling patterns form an entire cultural pattern. As we mentioned some pages before, tobacco smuggling has constituted one of the sources of financing of the AQIM even before it abandoned its earlier name (SGPC or Salafist Group for Preaching and Combat). In particular this was done by the katiba that as led until a short time ago by Mokhtar Belmokhtar who, not coincidentally, received the nickname of “Mr. Marlboro”44. Tobacco smuggling is probably the most lucrative form of trade of the many kinds that are practised in the region, above the smuggling of fuel, the arms trade and even drug trafficking45. Consequently, the gains extracted by AQIM by charging money to the tobacco smugglers that cross the Sahara desert should not be underestimated.

Lastly, the Iraqi scenario provides the best example concerning the involvement of jihadist elements in a variety of crimes geared towards fostering the fraudulent sale of fuel. According to data included in the Iraq Study Group Report, prepared during 2006 and presented to the United States Congress at the end of that particular year, between 15,000 and 200,000 barrels of oil, or perhaps many more, were stolen in that country every day during the first years of the conflict that began following the 2003 invasion46. The origin of that problem should be sought in the significant increase that the price of fuel underwent during those years due to budgetary restrictions and limitations on supply caused by the situation of conflict. The main consequence was the creation of a lucrative black market. All of the insurgents who were present in the country contributed towards this, without overlooking AQI or other jihadist militants. Besides controlling several of the distribution and exportation routes of oil and fuel, which made it possible to impose charges on the smugglers and sell protection to them, there are reports that demonstrate that some insurgent cells collaborated with certain companies created using illegal funds, whose bosses ended up being tried for having sold fuel that had been stolen from the Iraqi state at values that were higher than the market price47. In the same way, some of the attacks carried out by insurgents


45 DOWARD, Jamie, op. cit.


47 Oehme III, Chester G, op. cit.; WILLIAMS, Phil, op. cit.
against Iraqi oil distribution infrastructures could have been done with the aim of the corresponding cuts in the supply benefitting the particular black market in fuel.\(^{45}\)

4.3 Forms of collaboration

Almost all of the criminal activities that we have just highlighted as being perpetrated by jihadists have been undertaken against a backdrop of some degree of cooperation with the local criminal networks and organisations. In fact, the overall examination of the scenarios selected here shows an entire catalogue of alternative options of collaboration between terrorists and organised criminals. Whilst almost all of these have been pointed out to some extent in our previous comments, it seems timely to briefly explain the most significant options.

**Incorporation into the production chains related to illegal markets.** As we have already seen, the jihadist involvement in the drug business and in other unlawful trade has been made possible by their position of dominating the territories where these crops are grown or pass through. Nevertheless, this form of control can only be profitable if it translates into the setting up of a form of ongoing economic partnership with one or several of other groups involved in the same business. So for example, in order to make the most of the drugs business, the partners or former allies of Al Qaida in Afghanistan and Pakistan have had a kind of commercial relationship with the growers, professional traffickers, men of war and corrupt government officials. In the same way, in both Iraq and the Western Sahara, the jihadists have collaborated with smuggling networks.

**Tactical alliances.** Another form of collaboration that has more or less stayed the course consists of the formation of alliances or collaboration agreements with groups of professional criminals. Possibly the purest form of this way of working has taken place in the Sahara. In fact, and as several reports have borne witness to, the particular MOJWA jihadist organisation was created in 2011 as the result of a coalition that was formed at its outset by a combination of militants who had split away from AQIM and local criminal elements. This was possibly strengthened by the money that was contributed to it by Cherif Ould Taher and Mohamed Ould Ahmed, two powerful criminal bosses of the region, with long experience in drug trafficking and kidnappings.

**Sub-contracting of criminal services.** Imitating an increasing pattern of use within the general sphere of organised criminality, the jihadists that operate in several scenarios that are observed here have sub-contracted the services of criminal gangs and other people with illegal expertise in certain criminal activities, so as to economise on efforts or to avoid any other risk. Thus, in some occasions, the Iraq jihadists have

\(^{48}\) OEHME, III. op. cit.
commissioned purely criminal groups to kidnap some hostages for them. In turn, AQIM has paid some of the people associated with organised crime for them to act as intermediaries in releasing hostages. Going back to Iraq, besides bribing border officials, the jihadists in that country have hired local criminal gangs to obtain forged documents, together with the criminal networks established in neighbouring countries, who specialise in money laundering operations using fraudulent foundations.

*Opportunist transactions.* Finally, the terrorists have the possibility of taking advantage of specific opportunities for collaboration related to offers made by criminal gangs or to any unexpected change or event. To illustrate the former it is worth looking at the example of the hostages captured by several Iraqi criminal networks and who were then sold to the jihadists, without any request from the latter for them beforehand. As regards the second aspect, it is worth recalling the opportunities for buying weapons that unexpectedly become available because of the civil war that broke out in Libya in 2011 and the consequent ransacking of various arsenals of that country, whose deposits were partly used to halt the insurgents and terrorists of the Sahel.

4.4 Consequences of the interaction between terrorism and criminality in the three scenarios

The different forms of convergence between terrorism (or insurgent activity in general) and organised crime described above have had adverse repercussions at more than one level. The co-existence of both threats in Af-Pak, in the post-Saddam Hussein Iraq and in the Western Sahel has severely punished the local population, worsening the conditions of security in the extreme and exposing them to the risks of attacks, aggression, threats of the practice of extortion, theft, etc. In addition—and this could not be otherwise—the coincidence of terrorism and organised crime in the same scenario has caused harm to the economies of the countries and areas involved, raising security costs for the existing local businesses, increasing investment risks and, along more general lines, putting the brakes on all options for growth and economic development.

Going beyond the preceding human, social and economic repercussions, it is necessary to consider those of a political nature. This convergence has aggravated the particular institutional shortfalls which, from the outset, had stimulated and facilitated the terrorist, insurgent and criminal activities. Firstly, the substantial economic resources extracted by the jihadists and other insurgent factions, thanks to their involvement in illegal businesses and practices, have augmented the prevailing political instability at the same time. Second, the destabilising impact that is provoked by the terrorist and insurgent activity contributes towards deepening the problems of governability and repressive inefficiency that had existed before that. This serves to remove obstacles to the work of the criminal networks and organisations, and in this increases their opportunities for enrichment and provides incentives for them to collaborate with the terrorists and insurgents, so as to maintain the climate of instability and the repressive vacuum that they both take advantage of. This vicious circle, which at the time helped to prolong several of the internal liberating wars in Africa over the last days, has also
manifested itself in the jihadist focal points analysed in this section.

Lastly, the high degree of terrorist-criminal convergence attained in some failed parts of Afghanistan, Pakistan, Iraq and the Sahel strip also brings about adverse implications for global security. To start with, this convergence helps the regions affected to stay in contact with the movements of illegal activity that provide the resources to expanding transnational organised criminality: this is a type of criminality that the international bodies already consider to be a serious risk factor for peace, stability and global security. On the other hand, the empowerment of jihadi terrorism within the particular convergence scenarios simultaneously assists the expansion of that form of terrorism through different routes to the global scale: it spreads regionally, serving as an inspiration and stimulating jihadists groups and organisations from other latitudes and, finally, attracting and temporarily making use of foreign extremists and terrorists that are willing to fight and receive training, the orientation and support necessary so as to end up exporting the jihad to another part of the world.

5. Conclusions

The causal relationship set out in this paper is consistent with a gradual convergence between terrorism and organised crime. It can be asserted that in the best of cases, worldwide jihadist terrorism has not been unconnected with a certain degree of interaction with organised criminality, which actually spans all of the possible modalities and involves the different types of individuals and structures that provide the shape to the varied and changing morphology of the worldwide jihadist movement.

However, the examples that have been set out were chosen for their illustrative value, and not as cases that confirm a general pattern. For now, the structures selected do not exhaust the list of the individuals involved who are associated with global terrorism. With the information available to date, it cannot be confidently asserted that the overall situation of global terrorism is inevitably advancing towards a full and definitive convergence with organised criminality. In reality, while some of their representatives have collaborated closely with organised criminality, others have only done this in an isolated, sporadic or superficial way. Amongst other facts, we lack evidence about any manifestation of that convergence. But nothing should surprise us about this. Involvement in activities that are particular to organised crime may entail considerable risks and inconveniences for terrorists, with such them becoming discredited in the eyes of public opinion and their own social bases; the increase in the opportunities of being identified and located by security forces; possible infiltrations and betrayals; or finally, the “de politicisation” of their own militia. In most of the occasions in which

---

49 As regard the costs that are involved for terrorists in their involvement in criminal activities or their association with criminal organisations see: GUPTA, Dipak K. op. Cit.
terrorists turn to crime, they do so with the intention of financing themselves. However, insofar as other sources of financing that are not strictly illegal become available, it seems logical for the terrorists to opt to exploit these and avoid unlawful actions\(^5\). This has occurred, for example, with Al Qaida central itself, whose connections with criminality over the course of its history have been minimal\(^6\). In part, this characteristic may have been due to their capacity to gain access to money from legal investments and donations, and also to some extent to the need to develop their security measures. These include refraining from becoming involved in any activity that may draw the attention of those pursuing them, because it is illegal.

Our analysis also shows that not all of the options of criminal convergence are equally frequent within the sphere of global terrorism. Rather, direct and independent participation in criminal activities (confluence or appropriation of methods), both for the purposes of financing and logistics, is the preferred course of action, as compared to the less frequent collaboration with organised organisations and gangs. According to one argument that is worth corroborating, it is possible that the growing involvement of jihadist individuals in small-scale crimes in western country has been assisted by the proliferation of local cells or networks that are not subordinated to any of the leading and more powerful organisations related to global terrorism\(^7\). In any event, it seems that terrorists preferring acting with complete autonomy whenever possible, even when the carry out operations that are typical to organised criminality. A separate issue is to say that this is not always possible for them. Once again, we could consider security reasons as the most credible explanation for that preference. As regards the third type of convergence (hybrid blending or transformation), the examples of the evolution of terrorism towards conventional organised criminality, with the consequent deferral or abandoning of the particular political-religious agenda, are somewhat in the minority in the jihadist universe.

However, as we have indicated, the likelihood of terrorism and organised crime—in any of their forms—converging also depends on contextual factors. In fact, in the case of global terrorism, convergence has been seen to be much more frequent and significant in those parts of Central Asia, the Middle East and Western Africa, places where the structural or economic conditions have made it a financing option that is more lucrative, simple and opportune than any of the alternatives to this. This is demonstrated by the last sections of this paper, devoted to examining the experiences of convergence with organised crime that have been detected since the last decade of


\(^6\) DEL CID GÓMEZ, Juan Miguel. op. cit.; ROLLINS, John. WYLER, Liana Sun y ROSEN, Seth, op. cit.

the 2000's, in three geo-political spaces of greatest relevance for global terrorism, namely: the Af-Pak region, the post-Saddam Hussein Iraq and the Western Sahel. This examination shows it is in these places where the circumstances permit this and these stimulate the confusion of jihadist activism and organised crime that may reach extremes that are really dangerous.

In short, while the connection between global terrorism and organised criminality should not be assumed, de facto, it constitutes a genuine trend that is a cause for concern and is underway, which requires preferential treatment and attention. On the other hand, the problem of the critical scenarios would require specific and integrating interventions, based upon a greater level of cooperation between the national and multinational bodies and agencies that respectively have anti-terrorist and organised crime-fighting objectives assigned to them.
BIBLIOGRAPHY


National Court, Criminal Division, Second Section, Ruling no. 65/2007. Second Section Summary proceeding number 20/04 of the Central Magistrates Court no. 6, Division Roll no. 5/05.


DE LA CORTE, Luis and HRISTOVA, Hristina, “Papel de los tráficos ilícitos en el escenario Af-Pak” [Role of illegal trade in the Af-Pak scenario], Master document of the SISS, 3/2012. Available at: http://www.iecc.es


ESCOBAR STEMmann, Juan José, “Cómo luchar contra Al Qaeda” [How to fight Al Qaeda], Política exterior [Foreign policy], vol. 18, no 99, 2004, pp. 15-22.

Financial Action Task Force (FATF), Illicit Tobacco Trade, June 2012.


GUPTA, Dipak K., Understanding Terrorism and Political Violence, Nueva York, Routledge, pp. 146-160.


HOCINE, Boukara; MESSAOUD, Fenouche; LOTFI, Touatit; and KARIMA, Benhadj. “El terrorismo y sus enlaces con el tráfico de drogas en África subsahariana” [“Terrorism and its connections with drug-trafficking in sub-Saharan Africa”]. In SPANISH INSTITUTE OF STRATEGIC STUDIES (SISS) and MILITARY INSTITUTE OF DOCUMENTATION, EVALUATION AND PROSPECTS OF ALGERIA (MIDEP), “Terrorismo y tráfico de drogas en África subsahariana” [“Terrorism and drugs in sub-Saharan Africa”]. Work document of the Spanish Institute of Strategic Studies, 13/3/2013. Available at: http://www.iecc.es


JORDÁN, Javier, “Un estudio preliminar sobre las tendencias del terrorismo yihadista en Europa” [“A preliminary study on the trends of jihadist terrorism in Europe], Essays from the CESEDEN, 122, Ministry of Defence, Madrid, 2008, pp. 205-


PICARELLI, John and SHELLEY, Louise, “Organized Crime and Terrorism”, in J. Giraldo and Harold Trinkunas (eds.) Terrorist Financing and State Responses: A
Comparative Perspective, Stanford, Stanford University Press, 2007, p. 44.


Reinas, Fernando, “Un condominio yihadista en el norte de Mali: ¿cómo ha surgido?, ¿se consolidará? ["A jihadist establishment in northern Mali: how has it come about? Will it become consolidated? ]” Elcano Royal Institute, ARI 52/2012, 17/07/2012.


WANNENBURG, Gail, “Links Between Organised Crime and al-Qaeda”, South Af-


FIGHTING AGAINST ORGANIZED CRIME AND THE ACTION'S INFLUENCE ON THE NATIONAL SECURITY ENFORCEMENT

ALIN PAHONȚU

POLICE DEPARTMENT, SIBIU

ABSTRACT

Nowadays, the phenomenon of organized crime is drawing more and more attention from the part of the general public, national governments and international organizations. As the criminal groups get involved in the dangerous game of arm proliferation, illegal migration, governmental corruption and the penetration of global financial system — that is becoming more and more independent — organized crime is a threat to national, regional and global security. Through money laundering, corruption, the weakening of state institutions and the loss of confidence of citizens in the rule of law, organized crime is undermining the democratic and economic foundation of society. This thing lead to many heads of state calling to multilateral agreements, through which more powers and new duties would be given to the national authorities charged with countering organized crime.

Keywords
Organised Crime, National Security, Fighting Against Crime

More than two decades after the end of the Cold War, we can sadly see the fact that our expectations were not confirmed. After half of century of dangers, risks and security threats, that have been supported and developed on the basis of the numerous vulnerabilities raised by the ideological conflict supported by military means, there was a short-lived period of detente. In the euphoria of the moment, we have hoped that time had come for a better and safer world. Out of the opportunity window created,
there sprung a giant Pandora Box, which the international community has been struggling to close ever since.

The concept of security was a very controversial one, as it is shown by a 1986 UN study, made by a team of experts, concerning the "Concepts of Security" that has highlighted the existence of a limited conceptual similarity between these [1].

In our approach to national security, we keep in mind the way in which the state defines its national security problems, how it tries to solve them and how it defines its options.

The Explanatory Dictionary of the Romanian Language defines in a general way security as the fact of being sheltered against any danger, together with the existence of a feeling of trust and calmness inspired by the absence of any danger [2]. Security is associated therefore either with an individual either with a community perceived as a social organization. Community, in its turn, is determined by a series of traits, the most important among which is being part of a well-defined territory, in the sense of a house, city, region of a country (county or any other organizational form within a state), country, interstate region (with a total or partial coverage of the territories of the states) subcontinental or continental region and finally the world.

The issue of security is structured on different levels, depending on some criteria defined by the degree of cohesion of the groups in structures that have as a reference statal and inter-statal organization. Focusing on the state type of structure, to which the trait of national is also associated, there are two levels that stand out, according to the following type of security: national and international.

National security actually refers to the security of the state that encompasses in its boundaries the majority of the nation as well as the national minorities for whose security the state is responsible [3].

International security refers to groups of states that are in inter-conditioning relations from the perspective of their own security. Depending on the type of relations between two states (inexistent, diplomatic, alliance, association), we can talk about a collective security – in the case of political, economic, military alliances or about the security complex – where there is a group of states in which all the members of the group are strongly connected to the other members and at the same time, as group members, they are connected, to the states outside their group but in a lesser manner [4].

The analysis of data and information, specific to the main areas of the Romanian social and economic life that have been processed, have lead to the highlighting of some various genesis and motivation type of tensions, that trough their breadth or way of manifestation can turn themselves into serious risks for the stability of the public safety.

The economic reforms – the judicial reorganization of some companies, bankruptcy or abandon of activity profile of units from different areas of the economic activity have been accompanied by the aggravation of the state of frustration. On the basis of the deepening of the crisis, social unrest and uncertainty have been registered among the workers, which, in
order to promote their point of view, turn to rallies, protests, unauthorized meetings or blockings of headquarters and institutions buildings. Such type of situations occurred in the case of companies facing reorganization, in which the state hold some part of the shares, but that were mainly privately held from the sectors of heavy industry, car manufacturing industry, construction industry, mining industry or extraction industry.

The decisions of accelerating the privatisation process in the energy sector and establishing energy centres have influenced the social behaviour and have encouraged the tendencies of physical violence and aggressiveness among some workers and their families. Such situations have been registered in the case of people working in mining, metallurgy, energy industry, and which are constantly vulnerable of being subjectively manipulated or subject to partisan interests of disobeying the law.

In such domains like social protection, healthcare, education, and other state sectors there are still some manifestations of group or associate interests, partisanship goals and destabilization of some activities, which are many vulnerable points that can be unilaterally exploited by members of organized crime.

Under these circumstances, drug consumption can increase, as well as side activities like excessive alcohol consumption, violence, street begging, extortion and prostitution, as refutation elements, but which affect the public safety and the interests of the citizens.

Some ethnic or autonomization actions have affected the people and have turned themselves into risks for the local cohabitation of citizens and for the realization of their goals. Such type of attitudes are even accompanied by important ideologies in the country through obscure channels but also through the speeches of some persons and can lead to segregation, isolation, persecutions and eventually to direct interethnic violence.

In Romania there are important institutions of internal and international public law, diplomatic agencies, trade missions, regional organizations, branches, financial institutions or other type of institutions that are undertaking missions of special importance to our country, in a European, Euro Atlantic and consolidation of democracy context.

There are also tendencies to submit civil servants to the sphere of influence and domination of some well-known criminal group leaders, so that these can cover them up and avoid taking responsibility.

Other sources confirm the interests of some persons doing research for preparing their departure out of the country by using false documents that they try to obtain with the help of specialized personnel or by putting pressure upon law representatives by means of relatives or friends so as not to dispose of the means of law enforcement.

By making use of the situations already described, some members of organized crime are able to recruit new members, consolidate their power by evading the law, gather around group leaders for committing crimes that would enable them to make profit.

The persons that are in hardship are getting more and more vulnerable to the danger of being recruited for sexual exploitation and there are premises for the
internationalization of crime, alliances between organizations and transnational actions that can even have a terrorist imprint to them.

An area of interest for crimes can be consolidated in favour of some representatives of well-known organizations for their violent actions committed upon groups of people or for endangering goods and fundamental values, their members acting more easily when they find themselves in a situation of marginalisation or isolation.

We are not neglecting the context of the multiplying actions of some associative native groups of attracting new members in order to manipulate their thoughts and behaviour and to put them in situations of direct or indirect dependency towards their self-proclaimed spiritual leaders.

According to leading experts in the domain, at the present time there have been no situations with a high potential towards preparing or undertaking some terrorist activities, but the specialized authorities are keeping a close eye on some vulnerable situations that can degenerate towards such criminal actions.

The fraudulent use of some forms of capital and disguised financial investments can support some operations of acquiring assets and capital for some criminal bodies. That is why they are being closely checked by specialized bodies.

Out of their evaluations, we can draw the conclusion that the major danger and the predisposition for committing some extremely serious crimes comes from the part of various classes of extremist groups that are national citizens or foreigners, and that are able to commit some extremely cruel acts if they enhance their connexions and key points in Romania.

The end of the 20th century, marked by the fall of communism, meant the beginning of the process of lifting the iron curtain that had existed between the two systems, capitalism and socialism. These have favoured the appearance and evolution of the process of globalisation and consequently the setting and implementing of the principles of a new world order, but on the other hand, they also meant a kind of opening of the Pandora Box, by leaving a free road for the threats that had escaped the cage of the bipolar system.

In this context, the accession to the EU, the future accession to the Schengen area and the implicit establishment of the external borders of the EU on the current border of our country on the North, East and the shores of the Black Sea, are important steps in the process of socio-economic development on the European level as well as on a national level.

Being an extremely important gate towards Europe, Romania, through its geopolitical and geostrategic position, is experiencing increased pressures at its borders from the part of Organized crime. Among these there are, as we already mentioned, migration, in its two forms immigration and emigration, drug trafficking, human trafficking, arms trafficking, ammunition, explosive materials, stolen luxury cars trafficking, smuggling of goods (goods from the national cultural patrimony, counterfeited goods, cigarettes, alcoholic drinks, oil products, wood, drugs), illegal operation with banned goods on the entrance
on the territory of the country (radioactive waste, protected species of flowers and fauna, archaeological vestiges, rare rocks, illegal hunting and fishing). These are just some of the ways in which organized crime can act.

The specific risks are especially the enlarging of the area of attraction for the criminals, of the attempts of fraud of all types, smuggling and illicit traffic, the forming of international criminal networks that undertake a large and diversified rage of illicit acts using recent technical and technological means.

In the same category of risks to the state security there are the existence on the national territory of group made out of foreign citizens involved in illicit traffic and smuggling of various goods, the intensification of illegal transit and development of the internal market for drugs and illegal products, the changing of directions and entrance gates for drugs or other products from the West to the East, as well as transiting the territory through smuggling or illicit traffic of goods for the black market of some European states and outside this space.

The range of risks can be completed with border operations that breach the current legislation concerning consumer and environment protection, copyright protection, customs and commercial fraud, money laundering and fake foreign currency, speculation of legal provisions on the possibility of establishing companies with foreign trade activity in conjunction with gaps that are manifested in the abolition of ghost firms, incitement to extremism, intolerance, separatism or xenophobia, creating migration towards and out of Romania to Western countries as well as the development of international terrorism.

In my opinion, Romania is on the verge of passing from the status of transit country to that of target country for illegal immigration, drug traffic, luxury cars, arms and ammunition. The traffic and use of drugs have already found a fertile ground in the national criminal groups, but also outside them, as the number of drug addicts among young people is witnessing an alarming growth rate.

The use of fake or falsified ID cards, illegal traffic of persons in cargo compartments, attempts of corruption, blackmail and threats to the personnel working at the boarding crossings, intercepting the transmissions of confidential transborder data, diplomatic traffic, money laundering and evasion of customs or taxes or the collection of VAT returns for goods that did not actually crossed the border, together with numerical insufficiency of supervision and control personnel at the borders, a low level of training and equipment, the lack of practical skills, a low perspicacity of some of employees and many other things cause as many risks for transborder security.

If we extend the area of manifestation of the risks in the current situation, we can notice the existence of some new types of risks and threats with a direct bearing on the border security.

For example, political instability, manifested in some of the neighboring countries of Romania, characterized by the trespassing of human rights, ethnic and religious politicization, drives towards nationalism, extremism and fundamentalism, are causes of migrating fluxes that know no borders.
The diversity of forms of manifestation of these phenomena requires, in my view, rethinking the ways of countering, through a multicriteria forecasting and, consequently, their prevention, implementing measures for reducing vulnerability, increasing at the same time, the prompt response capability.

Simultaneously, it is to be expected that political and diplomatic relations, through specific means, will gain an essential role in preventing and combating all forms of manifestation of these transborder phenomena. Stability, security and justice are the valences of the world towards which we aim, a better and more prosperous world in which citizens may freely enjoy the democratic freedoms.

Organized crime caused the appearance of new policies, doctrines, strategies and countering tactics, but which, despite all efforts from the part of the democracies to deal with them, have not proven the effectiveness and efficiency expected from them. There is no doubt that cross-border crimes in their totality constitute an important component of organized crime, through their international character and as well as through the organizational manner and structure of the clusters they form. Usually, the element of strangeness has a clear role in the beginning, development or end of a criminal act.

In this context, a major danger that threatens the public order and the legality in the Romanian society is the strengthening of the degree of professionalism of criminal environments and structures of organized crime in particular.

It is well known that criminal groups made up in Romania are increasingly adopting the principles of organization, internal and hierarchical structures and especially the laws governing the mafia organizations, which have tentacles spread over most of the states of the world, like a true planetary octopus.

The most serious threat is that the primary goal of these organized crime groups is that of making the state structures in charge of carrying out social control and of fighting against them, ineffective, inefficient and even crippling, a goal that can be achieved by corruption or seizure of civil servants from the administration, police, justice, finance, through the means of which the organized crime groups influence the adoption or amendment of important decisions in the economic, legal domain etc.

Unfortunately, lately, there are increasingly more examples showing that the accountability of those responsible is extremely difficult, sometimes even impossible.

- We therefore naturally wonder: How should the guard, policeman or border guard look like in the following period? How or what should be changed in their education and training?

- The progress and pace of reforms is a matter which generally characterizes the Romanian society and structures of internal affairs can not be an exception in this respect.

- I believe that the structures fighting organized crime, according to the action and reaction principle, will have to deal especially with increasing the adaptability to changes in international environment characterized by a dynamics and mobility sufficient to make the changes or reform
effective after the threats have passed. The object of the transformations are these institutions themselves, that, through the process of structural compatibility and permanent, dynamic, practical and coherent adaptation can solve in optimal conditions the issue of specific crime phenomenon.

References

4. David, 68.
Terrorism and Transnational Crime: Foreign Policy Issues for Congress

John Rollins
Specialist in Terrorism and National Security

Liana Sun Wyler
Analyst in International Crime and Narcotics

June 11, 2013
Summary

This report provides an overview of transnational security issues related to patterns of interaction among international terrorist and crime groups. In addition, the report discusses the U.S. government's perception of and response to the threat. It concludes with an analysis of foreign policy options.

In recent years, the U.S. government has asserted that terrorism, insurgency, and crime interact in varied and significant ways, to the detriment of U.S. national security interests. Although unclassified anecdotal evidence largely serves as the basis for the current understanding of criminal-terrorist connections, observers often focus on several common patterns.

- **Partnership Motivations and Disincentives**: Collaboration can serve as a force multiplier for both criminal and terrorist groups, as well as a strategic weakness. Conditions that may affect the likelihood of confluence include demand for special skills unavailable within an organization, greed, opportunity for and proclivity toward joint ventures, and changes in ideological motivations.

- **Appropriation of Tactics**: Although ideologies and motivations of an organization may remain consistent, criminals and terrorists have shared similar tactics to reach their separate operational objectives. Such tactics include acts of violence; involvement in criminal activity for profit; money laundering; undetected cross-border movements; illegal weapons acquisition; and exploitation of corrupt government officials.

- **Organizational Evolution and Variation**: A criminal group may transform over time to adopt political goals and ideological motivations. Conversely, terrorist groups may shift toward criminality. For some terrorist groups, criminal activity remains secondary to ideological ambitions. For others, profit-making may surpass political aspirations as the dominant operating rationale. Frequently cited terrorist organizations involved in criminal activity include Abu Sayyaf Group (ASG), Al Qaeda's affiliates, D-Company, Kurdistan Worker's Party (PKK), Revolutionary Armed Forces of Colombia (FARC), Haqqani Network, and Hezbollah.

To combat these apparent criminal-terrorist connections, Congress has maintained a role in formulating U.S. policy responses. Moreover, recent Administrations have issued several strategic documents to guide U.S. national security, counterterrorism, anti-crime, and intelligence activities. In July 2011, for example, the Obama Administration issued the *Strategy to Combat Transnational Organized Crime*, which emphasized, among other issues, the confluence of crime and terrorism as a major factor in threatening the U.S. global security interests.

While the U.S. government has maintained substantial long-standing efforts to combat terrorism and transnational crime separately, Congress has been challenged to evaluate whether the existing array of authorities, programs, and resources sufficiently responds to the combined crime-terrorism threat. Common foreign policy options have centered on diplomacy, foreign assistance, financial actions, intelligence, military action, and investigations. At issue for Congress is how to conceptualize this complex crime-terrorism phenomenon and oversee the implementation of cross-cutting activities that span geographic regions, functional disciplines, and a multitude of policy tools that are largely dependent on effective interagency coordination and international cooperation.
Contents

Introduction .................................................................................................................. 1
Perceived Threat ........................................................................................................... 2
U.S. Government Strategies ......................................................................................... 4
Patterns in Crime-Terrorism Interaction ................................................................... 6
Partnership Motivations and Disincentives ................................................................. 6
Appropriation of Tactics ............................................................................................. 7
Violence for Political Effect ......................................................................................... 8
Crime-for-Profit ........................................................................................................... 10
Illicit Support Activity ................................................................................................. 12
Organizational Evolution and Variation .................................................................... 16
Abu Sayyaf Group (ASG) .......................................................................................... 17
Al Qaeda's Affiliates .................................................................................................... 17
D-Company .................................................................................................................. 18
Kurdistan Worker's Party (PKK) ................................................................................ 18
Revolutionary Armed Forces of Colombia (FARC) ................................................... 19
Haqqani Network ......................................................................................................... 20
Hezbollah ..................................................................................................................... 20
Foreign Policy Responses ........................................................................................... 21
Diplomacy ..................................................................................................................... 21
Foreign Assistance ....................................................................................................... 23
Financial Actions ......................................................................................................... 24
Intelligence ................................................................................................................... 25
Military Actions ........................................................................................................... 25
Investigations ............................................................................................................... 26
Looking Ahead: Implications for Congress ................................................................. 27

Tables

Table A-1. Foreign Terrorist Organization (FTOs): Reported Sources of External Aid ........ 30

Appendixes

Appendix. Terrorist Links to Criminal Financing ....................................................... 30

Contacts

Author Contact Information ......................................................................................... 35
Acknowledgments ......................................................................................................... 35
Introduction

Transnational terrorists and criminals may collaborate, appropriate shared tactics, and otherwise benefit from interaction, resulting in bolstered capabilities, enhanced organizational infrastructure, improved access to resources, and expanded geographic reach. Historical examples also indicate that terrorist and transnational criminal groups may evolve, converge, transform, or otherwise alter their ideological motivations and organizational composition to appear similar. Although information on the extent and nature of criminal-terrorist relationships, including their impact on U.S. national security, remains anecdotal, many view the potential confluence of criminal and terrorist actors, skills, resources, and violent tactics as a cause for concern.\(^1\) Such enhancements may in turn lengthen the duration of insurgencies, extend the longevity and capabilities of criminal and terrorist organizations, and undermine the ability of fragile governments to exert full control of their territory.

Some analysts have identified a series of potentially disturbing patterns that has hastened the expansion of relationships between terrorist and transnational crime groups. First, criminal syndicates appear to be growing in size, scope, and ambition. Globalization has extended their transnational reach, while major developments in technology, trade, and the financial industry have provided them with opportunities to exploit vulnerabilities in emerging criminal sectors, such as cybercrime. Many now maintain a transnational footprint and a flexible and networked membership roster that can adapt more readily to new market niches and establish more fluid alliances with external individuals and groups.

Second, the nature and activities of terrorist organizations appear to have also changed. Terrorist groups today, particularly those that most threaten U.S. global interests, appear to be motivated primarily by religious rather than nationalist and ethnic separatist imperatives that were common in the 1960s and 1970s. This shift has resulted in extremist movements that elicit sympathy well beyond a specific country or geographic region.\(^2\) Further, terrorist groups appear to have become more resilient, due to a combination of continued state sponsorship or support, as well as entrepreneurial expansion into profitable criminal activities.

Combined, these trends may suggest an increase in geographic overlap where criminals and terrorists could operate and interact. These patterns may also suggest greater blurring of distinctions between one group and the other, the adoption of activities often attributed to the other, or the ad hoc evolution of a group’s objectives based on the security challenges they encounter.\(^3\) Key nodes, where interaction is most likely, include prisons; cyberspace, particularly online opportunities for social networking; and ungoverned or difficult-to-govern spaces, which

---

\(^1\) This report is based on unclassified interviews and open sources. While the focus of this report is on threats to U.S. security interests manifested from terrorist organization-international organized crime syndicate partnering arrangements, it is important to note that the issue has garnered the attention of the wider international security community.


\(^3\) An action pursued with one set of motivations can evolve into a different scenario based on the challenges the terrorist or criminal actors encounter and the response of the host government and global security community. Some suggest that one example of such a transformation was the January 2013 attack on Algeria’s In-Amenas oil facility, where a kidnapping for ransom plot transformed into a hostage situation involving violence-based terrorist tactics. Notably, the attack was reportedly masterminded by Moktar Belmoktar, an illicit actor with longstanding ties to both Islamist groups and organized crime.
include regions plagued by endemic corruption, conflict or post-conflict zones where legitimate governance has yet to take root, border regions, free trade zones, and urban mega cities where pockets of poverty, violence, criminality, and impunity from national law prevails. Overlap may also be facilitated by the involvement of negligent or hostile governments and kleptocratic or criminal states that may consider sponsorship or support of criminal or terrorist activity of strategic value.

Perceived Threat

The U.S. government has asserted that terrorism, insurgency, and crime interact in varied and significant ways, to the detriment of U.S. national security interests. In January 2012, the Director of National Intelligence (DNI) reported to Congress that transnational organized crime and its links to international terrorism was among the nation's most pressing national security concerns, specifically identifying the following areas of concern for crime-terrorism interaction:

- **Nuclear proliferation:** "We are aware of the potential for criminal service providers to play an important role in proliferating nuclear-applicable materials and facilitating terrorism."

- **Kidnapping for ransom:** "Kidnapping for ransom is increasing in many regions worldwide and generates new and deep income streams for transnational criminal networks ... and terrorist networks."

- **Human smuggling:** "Those who smuggle humans illegally have access to sophisticated, forged travel papers and the ability to constantly change their smuggling routes—routes that may span multiple continents before reaching their destinations. Smugglers undermine state sovereignty and sometimes facilitate the terrorist threat."

- **Illicit finance:** "Terrorists and insurgents will increasingly turn to crime and criminal networks for funding and logistics, in part because of U.S. and Western success in attacking other sources of funding. Criminal connections and activities of both Hizbollah and AQIM [Al Qaeda in the Islamic Maghreb] illustrate this trend."

DNI James R. Clapper's testimony to Congress in 2012 reiterated the findings of the U.S. intelligence community's 2010 review of threats posed by transnational organized crime. In that review, the first of its kind in 15 years, the intelligence community ultimately concluded that such illicit networks have “dramatically” increased in size, scope, and influence internationally. A public summary of the assessment identified a “threatening crime-terror nexus” as one of five key threats to U.S. national security:

Terrorists and insurgents increasingly will turn to crime to generate funding and will acquire logistical support from criminals, in part because of successes by U.S. agencies and partner nations in attacking other sources of their funding. In some instances, terrorists and insurgents prefer to conduct criminal activities themselves; when they cannot do so, they turn to outside individuals and facilitators. Proceeds from the drug trade are critical to the

---

continued funding of such terrorist groups as the Taliban and the Revolutionary Armed Forces of Colombia (FARC). Terrorist organizations such as al-Shabaab and drug trafficking organizations such as the cartels based in Mexico are turning to criminal activities such as kidnapping for ransom to generate funding to continue their operations. Some criminals could have the capability to provide weapons of mass destruction (WMD) material to other terrorist groups, such as Hizballah and al-Qa'ida in the Islamic Maghreb, though the strength of these drug links and support remain unclear. U.S. intelligence, law enforcement, and military services have reported that more than 40 foreign terrorist organizations have links to the drug trade. Some criminal organizations have adopted extreme and widespread violence in an overt effort to intimidate governments at various levels.5

DNI Clapper’s testimony to Congress in 2013 additionally noted that the U.S. intelligence community is “monitoring the expanding scope and diversity of ‘facilitation networks,’ which include semi-legitimate travel experts, attorneys, and other types of professionals, as well as corrupt officials, who provide support services to criminal and terrorist groups.”6

Other U.S. government documents characterize the confluence of transnational organized crime and international terrorism as a growing phenomenon. Whereas in previous decades criminal and terrorism links occasionally occurred, such connections appear to be taking place with greater frequency today and may be evolving into more of a matter of practice rather than convenience. According to the U.S. Department of Justice (DOJ), recent investigations suggest that international organized criminals are willing to provide logistical and other support to terrorists.7 According to the U.S. Drug Enforcement Administration (DEA), 19 of 49 (39%) State Department-designated foreign terrorist organizations (FTOs) have “confirmed links to the drug trade” as of November 2011.8 In 2003, DEA reported that 14 of 36 (39%) FTOs were involved “to some degree” in illicit narcotics activity.9 For FY2010, DOJ reported that 29 of the top 63 international drug syndicates, identified as such on the consolidated priority organization target (CPOT) list, were associated with terrorists.10

The State Department’s 2012 Country Reports on Terrorism describes more than 20 FTOs as having financially profited from criminal activity to sustain their terrorist operations (see the Appendix).11 Such listed FTOs include Al Shabaab, Army of Islam (AOI), Al Qaeda in the Arabian Peninsula (AQAP), Al Qaeda in Iraq (AQI), Al Qaeda in the Islamic Maghreb (AQIM), Abu Sayyaf Group (ASG), United Self-Defense Forces of Colombia (AUC), Continuity Irish Republican Army (CIRA), Communist Party of the Philippines (CPP), Revolution People’s

---


Liberation Party (DHKP/C), National Liberation Army (ELN), Revolutionary Armed Forces of Colombia (FARC), Moroccan Islamic Combatant Group (GICM), Hamas, Hezbollah, Haqqani Network (HQN), Jemaah Ansharut Daulah (JAD), Jemaah Islamiya (JI), Lashkar i Jhangvi (LJ), Liberation Tigers of Tamil Eelam (LTTE), Kurdistan Workers’ Party (PKK), Shining Path (SL), and Tehrik-e Talib Pakistan (TTP).

Such government studies reinforce assessments from the late 1990s that predicted an increase in crime-terrorism interactions. For example, in 1997, a U.S. Department of Defense (DOD) task force study on transnational threats concluded that terrorists groups, religious extremists, anti-government militias, narcotics traffickers, and global criminals were “increasingly linked in new and more cooperative ways.” In 2000, a U.S. interagency assessment of international crime threats further highlighted growing crime-terrorism interactions. The assessment identified the end of the Cold War as a major contributor to this development. As certain insurgent and extremist groups were no longer able to rely on Soviet-affiliated state sponsors for aid, some increasingly turned to crime as an alternative source of funds. The assessment also concluded that most crime-terrorism interactions were often fleeting, or based on symbiotic arrangements that were nevertheless strained and marked by suspicion. Some groups, however, viewed criminal activity as not only a lucrative source of funding, but also an effective means to advance their political or ideological objectives. Other groups, meanwhile, underwent transformations in which their primary organization motivations would shift from political to (illicit) profit-driven.

U.S. Government Strategies

To combat this apparent criminal-terrorist connection, recent Administrations have issued several key strategic documents to guide U.S. government efforts and approach the issue from the perspectives of national security, counterterrorism, anti-crime, and intelligence. The Obama Administration’s key strategic documents are described below in chronological order.

In August 2009, the Obama Administration issued its National Intelligence Strategy, which included as a primary mission the goal of penetrating and supporting “the disruption of terrorist organizations and the nexus between terrorism and criminal activities.”

In May 2010, the Obama Administration issued its National Security Strategy, a broad-ranging document that identified key priorities for the United States. One such priority was to combat “transnational criminal threats and threats to governance”—including the “crime-terror nexus.”

15 The report states that some groups, particularly those that controlled territory, would encourage illicit activity in the region to “isolate” it from the national economy, to “deprive the government of the region’s economic productivity,” and to “increase the dependence of the local population on their control and authority.”
The 2010 National Security Strategy encouraged a “multidimensional strategy” that emphasized citizen security and harm reduction, disruption and dismantling of illicit networks, and bolstering the capacity of foreign governments to enforce the rule of law.

In April 2011, the U.S. Department of Defense (DOD) issued a Counternarcotics and Global Threats Strategy. The strategy describes an international security environment characterized by a “confluence of dispersed and decentralized global networks of criminals and terrorists.” It further states that such networks are “composed largely of individuals and groups that receive occasional support from corrupt government officials” and “are loosely organized and ever-evolving, pragmatically appearing and disappearing for political-criminal gain.” The DOD strategy identifies three strategic goals:

- to disrupt and disable actors and activities related to trafficking, insurgency, corruption, threat finance, terrorism, drug precursor chemical distribution in Afghanistan and Pakistan;
- to sharply reduce illicit drug and drug precursor chemical distribution, as well as related transnational organized criminal threats in the Western Hemisphere, particularly Mexico, Central America, Colombia, and Peru; and
- to mitigate the size, scope, and influence of targeted transnational criminal organizations and trafficking networks such that they pose only limited, isolated threats to U.S. national and international security.

In June 2011, the Obama Administration issued its National Strategy for Counterterrorism. Included among its eight “overarching goals” was the goal to “deprive terrorists of their enabling means”—terrorist financing and the facilitation of terrorist travel, materiel smuggling, and communications. The Administration’s National Strategy for Counterterrorism sought to achieve this goal by

- blocking the flow of financial resources to terrorist groups through sanctions, prosecutions, international cooperation, and diplomatic pressure (money laundering and kidnapping for ransom); and
- working with international partners to identify and prevent terrorist groups from moving its recruits, operatives, and supplies across borders (human and weapons smuggling).

In July 2011, the Obama Administration issued its Strategy to Combat Transnational Organized Crime. Among its primary objectives was to “defeat transnational criminal networks that pose the greatest threat to national security by targeting their infrastructures, depriving them of their enabling means, and preventing the criminal facilitation of terrorist activities.” Key actions described by the strategy to combat the crime-terrorism nexus included the following:

---

19 Order of countries and regions as stated in the original text.
20 Obama Administration, National Strategy for Counterterrorism, June 2011.
• Enhancing intelligence collection on transnational organized crime threats, particularly the potential role of criminal groups in facilitating WMD terrorism.

• Exposing vulnerabilities in the international financial system that could be exploited by “terrorist and other illicit financial networks” and applying financial tools and sanctions against such networks.

• Establishing a “whole-of-government plan” to combat kidnapping for ransom as a means to finance terrorists, among other “bad actors.”

• Developing a “comprehensive approach” to dismantling drug trafficking organizations with connections to terrorist groups.

• Enhancing foreign capabilities through counterterrorism capacity building, foreign law enforcement cooperation, military cooperation, and the strengthening of justice and interior ministries.

Patterns in Crime-Terrorism Interaction

Limited unclassified anecdotal evidence largely serves as the basis for the current understanding of criminal-terrorist connections. In the absence of comprehensive data, it is difficult to assess whether such anecdotal cases are indicative of a widespread problem, a growing trend, or isolated observation. What is clear from existing literature on the subject, however, is that crime-terrorism interactions can vary significantly and change over time. The following sections summarize several common patterns of crime-terrorism links, with specific examples drawn from a range of court cases, reports, and news articles.

Partnership Motivations and Disincentives

The underlying rationales for criminal and terrorist group partnerships as well as the conditions that may facilitate the evolution or transformation of a criminal or terrorist group into the other may vary. Collaboration can serve as a force multiplier for both criminal and terrorist groups, bolstering their capabilities, strengthening their infrastructure, and increasing their wealth. On the other hand, partnering could also have the potential of sowing seeds for distrust and competition among illicit actors—vulnerabilities that could be exploited by international security authorities.

From the perspective of a terrorist organization, the primary motivation for partnering or adopting criminal tactics would be to sustain and grow the organization for purposes of pursuing or financing its ideological-based activities. Out of this sense of perceived need, the organization may turn to or rely more heavily on partnering with criminal syndicates for continued viability. Common disincentives for partnering would include increased attention from government authorities; fear of compromising internal security; ideological resistance to illicit endeavors; and the availability of sufficient alternative funding sources, such as state sponsors.


Such considerations are predicated on the theory that the leaders of an organization think rationally about the near- and long-term considerations and consequences, unintended or otherwise, of partnering with an entity that has differing motivations and ideologies.
From the perspective of a criminal syndicate, motivations for cooperating with terrorist organizations would include the near singular purpose of increasing its financial stature. As with terrorist organizations, common disincentives from the perspective of criminal groups may involve increased and unwanted attention from authorities, risk of infiltration, and heightened vulnerability of organization leadership to capture. Criminal groups already in control of lucrative revenue streams may not find the potential for additional business with terrorist groups sufficient to outweigh the costs. Criminal groups may also opt to avoid collaboration with terrorist groups if such interactions would disrupt their relationships with corrupt government officials who are willing to facilitate criminal activities, but not terrorism-related ones.

Conditions that may affect the likelihood of confluence include a lack of in-house capabilities and demand for special skills to conduct particular operations. Some groups may be more hesitant to collaborate with outsiders, depending in part on the nature of the operational environment, the presence of competitors, and the opportunity for contact with and the strength of relations between terrorist and criminal elements. Other barriers to cooperation may include cultural, religious, or ideological differences across groups. On the other hand, motivations such as greed or necessity for organizational viability or expansion may induce some groups to welcome or seek out external partners.

Individual groups may also transition along an apparent crime-terrorism continuum. Over time, ideologically motivated groups that initially avoid involvement with criminal activities may become increasingly attracted by the lucrative nature of criminal activities. In other instances, criminal groups may become radicalized and apply their criminal expertise to conduct operations that not only result in lucrative illicit profits but also further ideologically oriented goals. In other situations, individuals in a terrorist organization may not follow leadership directives to stay away from individuals in a criminal organization (or vice versa) and may unilaterally develop external relationships. Some analysts suggest that this phenomenon may occur with greater regularity due to the increasingly decentralized nature of terrorist groups and other possible factors.

Appropriation of Tactics

Criminals and terrorists often share similar tactics to reach their operational goals. These include acts of terrorism and political violence; involvement in criminal activity for profit; money laundering; undetected cross-border movements; illegal weapons acquisition; and government corruption. Changes in the selection of tactics may signify shifts in the strength and capacity of an organization or the ideological desires of the organization's leadership. A criminal group under pressure by authorities or rival criminal groups may react by organizing violent attacks to intimidate the public and deter the government from future pursuit. A terrorist group's loss of state sponsorship may prompt it to find illicit alternatives for funding and operational support. The following sections describe several methods and tactics common to both criminal and

---


26 It should be noted that the adoption of a tactic by either a criminal or terrorist group that is traditionally used by the other entity in and of itself does not change the ideology, motivation, and goals of the organization or how it might be designated and approached by international security actors.
terrorist groups, including (1) the use of violence for political effect, (2) crime-for-profit activities, and (3) illicit support activity.

**Violence for Political Effect**

Although more commonly associated with terrorist groups, criminal groups have also occasionally used violence as a tactic to change political and public perceptions. Common past examples have included the use of terrorist-style violence, intimidation, and hostage-taking tactics by the Brazilian prison gang and drug trafficking organization (DTO) Primeiro Comando da Capital (PCC) in 2006. In response to counternarcotics pressure in the 1980s and 1990s, the Medellin cartel conducted a wave of violent attacks on Colombian government and civilian targets, including the explosion of a commercial airliner and a truck bomb. The Italian mafia targeted prominent landmarks, politicians, and government officials in response to law enforcement pressure in the 1990s.

Drug trafficking-related violence in Mexico, which surged in recent years due to a combination of increased counternarcotics pressure by the government and DTO-on-DTO competition, has at times appeared similar to terrorist-style attacks, with comparable tactics of intimidation. Mexican government officials, for example, have been targeted by traffickers, at times in reprisal for their role in cartel arrests. In May 2008, one of Mexico's highest-ranking law enforcement officials, Edgar Millan Gomez, was assassinated in Mexico City by DTO-affiliated gunmen. In other cases, drug traffickers have deployed small improvised explosive devices (IEDs) against law enforcement officials suspected of working for rival gangs.

Observers continue to debate whether the use of political violence as a tactic by Mexican DTOs warrants describing such groups as terrorist organizations. Most observers recognize that few instances of Mexican DTO violence appear to be motivated by ideology or a desire to overthrow the Mexican government. According to the State Department's 2012 Country Reports on Terrorism, there was “no evidence that these criminal organizations had political or ideological motivations, aside from seeking to maintain the impunity with which they conduct their criminal activities.” Some have suggested that one of these exceptions may have occurred in September 2008, when a deadly attack on Mexico’s Independence Day involving throwing grenades into a crowd of revelers that had gathered for a firework display was suspected to have been organized.

---


by drug traffickers. Yet, in this case, some traffickers appeared to distance themselves from the attack, joining in the victims’ outcry and refusing to take responsibility for the attack. Other incidents that have raised questions about Mexican drug traffickers’ motives and tactics include a casino fire that killed 52 civilians in 2011, and was allegedly instigated by Los Zetas.

---

The Suspected 2011 Iranian Plot to Assassinate the Saudi Ambassador to the United States

Highlighting the potential for cooperation among organized crime and terrorist groups to plan and conduct an act of violence is the alleged plot to assassinate Saudi ambassador to the United States Adel al-Jubeir, publicly disclosed in October 2011. According to U.S. authorities, Mansoor Arbabshar, a dual U.S.-Iranian national from Corpus Christi, TX, and several members of the Iranian Revolutionary Guards Corps-Quds Force (IRGC-QF) planned to assassinate al-Jubeir by bombing a local restaurant he frequented and also by bombing the Saudi Arabian and Israeli embassies in Washington, DC.

As part of the alleged bombing plot, Arbabshar arranged to hire members of the Mexican DTO Los Zetas to conduct the assassination for a fee of $1.5 million. A side deal was reportedly discussed in which several tons of opium from the Middle East would be trafficked to Mexico. The alleged plot, however, was discovered because Arbabshar’s Mexican DTO intermediary was in fact an informant for the DEA. Arbabshar was ultimately arrested in New York and reportedly confessed to having been recruited, funded, and directed by the IRGC-QF to find Mexican DTO members to conduct the assassination plot. In conjunction with Arbabshar’s arrest, the U.S. Department of the Treasury announced financial sanctions against Arbabshar and others connected to the plot who were alleged members of the IRGC-QF, an organization that the Treasury Department had designated pursuant to Executive Order (EO) 13224 in October 2007. On October 17, 2012, Arbabshar pleaded guilty in U.S. federal court to charges associated with the murder-for-hire plot. In announcing the guilty plea, DEA Administrator Leonhart noted, “The dangerous connection between drug trafficking and terrorism cannot be overstated.” On May 30, 2013, Arbabshar was sentenced to 25 years in prison.

Many observers have commented with incredulity that the IRGC-QF would partner with a non-Muslim DTO or use non-professional Iranian-American operatives such as Arbabshar, and that senior Iranian authorities would authorize such an action on U.S. soil. It remains to be seen whether this alleged plot is indicative of greater crime-terrorism cooperation or a one-time departure from conventional IRGC-QF tactics. Other alleged plots, many of which appear to have also failed spectacularly, have been attributed in media reports to other Iranian sponsored groups, including Hezbollah.

---


37. Ibid.

Crime-for-Profit

In addition to organized crime groups, some terrorist organizations may seek funding through criminal activities. Often, the potential profits associated with criminal activity are a motivating factor for both organized crime and terrorist groups. Since the end of the Cold War and corresponding declines in traditional state-sponsored sources of funding, some observers suggest that terrorist groups have become increasingly motivated to generate funds through criminal activity to sustain organizational capabilities. Heightened international counterterrorism measures in the past decade may have further depleted other traditional sources of funds, including private sector donations, which reinforce the desire for terrorist groups to seek alternative funding methods.

Criminal activities conducted for profit may range from local crimes of theft, burglary, and extortion to illicit trafficking of high-value commodities on a transnational scale. Terrorist groups may also "tax" other groups or charge a security or protection fee for permitting illicit trafficking activity to take place in a certain region under their control. Although terrorist groups may engage in criminal activity for fundraising, it is not always the case that such groups lose their ideological motivations. As one researcher explains, "[C]riminality does not imply criminalization. It is entirely possible for armed groups to exploit drugs, smuggling, and extortion without becoming motivated by these activities. Resources do not speak for themselves; simply engaging in criminality does not mean that an armed group exists to be criminal."39

The universe of potential crime-for-profit activities is vast. The following list describes three common transnational manifestations: drug trafficking, cigarette smuggling, and kidnapping-for-ransom.

- **Drug trafficking:** Illicit narcotics, particularly cocaine, heroin, hashish, and methamphetamine, as well as the chemical precursors required to manufacture such drugs, are attractive commodities to smuggle due to their high pecuniary value, as well as the ease with which they can be appropriated, processed, stored, and transported in small, difficult-to-detect movements and with limited static infrastructure costs. Terrorist groups are associated with major drug-producing countries, such as Afghanistan, Burma, Colombia, Morocco, and Peru, as well as among countries through which key drug transit routes pass.40 In drug-producing countries, the narcotics trade has the potential to provide terrorist groups with an added bonus: recruits and sympathizers among impoverished, neglected, and isolated farmers who can not only cultivate drug crops but also popularize and reinforce anti-government movements.41

---


Afghan Drugs and the Taliban

As the single largest source of illicit opium and heroin worldwide for the past decade, the narcotics trade is both a major cause and consequence of criminality and insecurity in Afghanistan. Although historically not always the case, the opiate trade today appears to be one of several key sources of funds for the Taliban. According to the U.N. Office on Drugs and Crime (UNODC), Afghan opiates generated approximately $68 billion in proceeds in 2009, of which some $140 million-$170 million went to anti-government insurgency groups, such as the Taliban. U.S. reports further indicate that some of the Taliban’s narcotics proceeds have been funneled in and out of Afghanistan and countries in the Persian Gulf through hawala-style informal value transfer networks and money exchanges houses, such as the New Ansari Money Exchange.

Research indicates that the Taliban reportedly obtains drug-related proceeds in several ways. Taliban commanders reportedly collect agricultural tithes (ushr) from poppy farmers and roadside levies (zokat) from traffickers. Additionally, the Taliban reportedly receives money, vehicles, and weapons in exchange for protection against interdiction and eradication. The Taliban also supports efforts to facilitate seasonal migrant flows toward opium poppy farms for harvest. Opium traffickers pay the Taliban to transport narcotics throughout Afghanistan to neighboring nations. Moreover, Taliban fighters appear to provide security for processing labs and for shipments of the chemicals needed to make heroin. They also help drug lords fight Afghan government forces engaged in poppy eradication efforts. Moreover, local Taliban commanders have at times directly engaged in drug trafficking activities to supplement their incomes.

- **Illicit tobacco trade**: The production, smuggling, and sale of tobacco products, including genuine and counterfeit cigarettes, is a lucrative form of financing for organized crime as well as terrorist groups, such as Hezbollah, Hamas, the Kurdistan Worker’s Party (PKK), and the Real Irish Republican Army (RIRA).

---


Cigarette smuggling schemes as a means for financing terrorists have been discovered in a range of countries and regions, including the United States, Europe, Turkey, the Middle East and North Africa, and Iraq. Criminals and terrorists may be drawn to the illicit tobacco trade to take advantage of price differentials across jurisdictions, bootlegging small consignments from a low-tax or duty-free outlet and re-selling the products elsewhere at a higher price. If sufficiently resourced, some groups may conduct larger-scale operations that divert and smuggle commercial-sized volumes, those in excess of 1 million cigarettes per consignment, for subsequent distribution and sale.

- **Kidnapping for ransom**: A form of hostage taking, kidnapping for ransom (KFR) is a popular means of collecting illicit profits for both organized crime as well as terrorist groups. KFR is often perceived as a crime of low risk, low cost, and high reward. As has reportedly been the case for groups such as AQIM, AQI, the Taliban, and ASG, a single ransom payment has the potential to cover several months of operating expenses. According to the Financial Action Task Force (FATF), AQIM alone has collected at least $65 million (U.S. dollars) in KFR payments from 2005 through 2011—a significant portion of its annual budget, which is reported to total approximately 15 million Euros per year. Authorities are particularly challenged to respond to KFR situations because they often take place in insecure, politically volatile locations that are difficult to control or access; involve third-party intermediaries who may facilitate negotiations of ransom payments without the approval and knowledge of government officials; and are characterized by opaque and difficult-to-track ransom payment transactions that involve both alternative remittance mechanisms and the formal international banking system.

## Illicit Support Activity

Both criminal and terrorist groups rely on a variety of illicit support activities to further their operations. Although some such activities can be conducted with in-house capabilities and assets, others may require cooperation with external criminal specialists, corrupt “gatekeepers,” local and regional “fixers,” and “shadow facilitators.” The depth and durability of these crime-

(...continued)


terrorism relationships for support activities vary. Some terrorist groups view links to outside criminal networks as short-term marriages of convenience, where the actors build ephemeral business ties. These interactions often appear to be distinctly transactional in nature, with one criminal actor or organization providing a specific, tangible service to a terrorist group. In other cases, these relationships will be more synergistic, with terrorist and criminal groups creating enduring coalitions. In such coalition relationships, criminals and terrorists assume complementary but separate roles.

- **Money laundering:** Illicit support activities may include money laundering techniques to obfuscate the origins and recipients of funds through front companies, charities, shell corporations, and other third-party business structures. The movement and storage of money may also involve illicit support activities such as bulk cash smuggling and cash couriers; the exploitation of informal remittance mechanisms, international trade systems, and the formal international banking sector; and the use of unregulated diamonds, gold, and other minerals and commodities for stored value.\(^4\)

---

\(^4\) GAO, *Terrorist Financing...*, November 2003; Rabasa et al., “Chapter Seven: The Convergence of Terrorism...,” 2006. In the late 1990s and early 2000s, Al Qaeda purportedly used illegal diamond trade in Africa as a means of stored value transfer and as part of gems-for-weapons deals.
Hezbollah, Narcotics, and Illicit Finance: Global Interactions

Hezbollah is a Shi'ite Islamist militia, political party, and social welfare organization, as well as a State Department-listed FTO and a specially designated terrorist group pursuant to EOIs 12947 and 13224.55 According to official U.S. government statements, it derives financial benefits from a sprawling global commercial network of illicit and illicit businesses that not only generates revenue for the organization but also provides numerous outlets through which illicit funds can be laundered, disguised, and moved (see also the “Hezbollah” section below, under “Organizational Evolution and Variation”). Although anecdotal reports have long appeared to connect Hezbollah global operations with drug trafficking, money laundering, and other illicit activity, several recent cases in 2011 have highlighted the potential transnational reach of Hezbollah’s illicit finance activities.56

In February 2011, the Treasury Department’s Financial Crimes Enforcement Network (FinCEN) designated Lebanese Canadian Bank SAL as a financial institution of primary money laundering concern pursuant to Section 311 of the USA PATRIOT Act (31 U.S.C. §318A). In its public notice on the Section 311 finding, FinCEN described the Lebanese Canadian Bank SAL as “routinely used by drug traffickers and money launderers operating in various countries in Central and South America, Europe, Africa, and the Middle East” and that Hezbollah profited from the criminal activities of this global illicit financial network.57

Central to the designation were law enforcement and other sources of information that linked the Colombia-based narcotics trafficking kingpin Ayman Joumaa with a global network involving Hezbollah facilitators, such as Ali Mohamad Saleh, and other linked money laundering operations, including those controlled by Jorge Fadallah Cheaitelly and Mohamad Zouheir El Khansa.58 In January 2011, the Treasury Department designated Joumaa as a drug kingpin (SDNTs) and additionally identified him as a specially designated global terrorist (SDGT) in June 2012. In December 2011, Joumaa was also indicted on drug charges in the United States. According to such charges, he allegedly coordinated cocaine shipments in connection with the Mexican DTO Los Zetas and laundered as much as $200 million per month through accounts held with Lebanese Canadian Bank SAL and other financial institutions.59

His South and Central American drug trafficking operations shipped cocaine to the United States and well as to West Africa for further distribution to Europe. Joumaa reportedly paid undisclosed fees to Hezbollah to facilitate the transportation and laundering of narcotics proceeds. For example, for bulk cash movements through Beirut International Airport, Joumaa paid Hezbollah security to safeguard and transport cash.

Joumaa also reportedly used trade-based money laundering (TBML) schemes to help conceal and disguise the true source, nature, ownership, and control of the narcotics proceeds. Such schemes involved Asian suppliers of consumer goods as well as used car dealerships in the United States. As part of the U.S. car sales-TBML scheme, for example, Hezbollah owned and controlled funds are transferred from Lebanon to the United States via banks, currency exchange houses, and individuals in order to purchase used cars. The cars would be shipped to West Africa and sold for cash. Cash proceeds, in turn, would be transferred to Lebanon through Hezbollah-linked bulk cash smugglers, hawaladars, and currency brokers.

Hezbollah’s contacts in West Africa make this region in particular an attractive mid-point for exchanging contraband and cash and connecting with like-minded, ideologically driven criminals. In another recent U.S. narcotics trafficking case, for example, a West Africa-based criminal facilitator and member of the Free Patriotic Movement, a Lebanese Christian party aligned with Hezbollah in the Lebanese cabinet, reportedly provided extensive services to Hezbollah. According to his indictment, Maroun Saade would pay local bribes to release Hezbollah’s cash couriers who were arrested in West Africa.60 In the DEA-led operation that ultimately caught Saade and several of his associates, he agreed to provide individuals whom he thought were Taliban (though were in fact DEA confidential sources) with cocaine in exchange for weapons and heroin.

55 For more on Hezbollah see CRS Report R41446, Hezbollah: Background and Issues for Congress, by Casey L. Addis and Christopher M. Blanchard.
IIlicit movements of people, arms, and equipment: Other common forms of illicit support activities include the clandestine movement of people and the acquisition of materiel and communications equipment—all of which also require access to a variety of fraudulent international documents, including visas, passports, and user certificates, business registrations, shipping licenses, etc. In one example, based on research conducted by the RAND Corporation and press reports, the Liberation Tigers of Tamil Eelam (LTTE) apparently maintain a cadre of criminal intermediaries for procuring and smuggling weapons. Such affiliations between arms brokers and the terrorist group appear to have been purposefully indirect in order to maintain sufficient distance between criminal activities and the leaders of the Tamil Tigers. In another example, a traditional human smuggling network along the Syrian-Iraqi border was transformed by AQI into a key pathway used by foreign terrorists to clandestinely enter Iraq.

(...continued)


59 U.S. District Court, Eastern District of Virginia, United States of America v Ayman Joumna, indictment, November 23, 2011; U.S. District Court, SDNY, United States of America v Lebanese Canadian Bank SAL et al., complaint, December 15, 2011.

60 U.S. District Court, SDNY, United States of America v Maroun Saade et al., indictment, unsealed February 14, 2011.


63 According to press accounts, Abu Ghadiyah (now deceased) and his family were reportedly long known to the U.S. intelligence community as a human smuggling operation along the Syrian-Iraqi border. Around the time when U.S. forces invaded Baghdad in 2003, Abu Ghadiyah transformed his traditional smuggling operation into a key Al Qaeda in Iraq (AQI) hub for logistics and financial support—including provisions of passports, weapons, money, guides, and safe houses—to foreign terrorists seeking entry into Iraq. According to the Treasury Department, Abu Ghadiyah was appointed in 2004 as AQI’s Syrian commander of logistics. In this position he not only continued his smuggling activities but also reportedly became involved in organizing at least two attacks in Iraq. See Mark Hosenball, “Targeting a ‘Facilitator’: A Commando Raid into Syria Aimed at Al Qaeda in Iraq,” Newsweek, October 27, 2008; U.S. Department of the Treasury, “Treasury Designates Members of Abu Ghadiyah’s Network: Facilitates Flow of Terrorists, Weapons, and Money From Syria to al Quida in Iraq,” press release, February 28, 2008; Matthew Levitt, “Al-Qaida’s Finances: Evidence of Organizational Decline?” CTC Sentinel, CTC at West Point, Vol. 1, Issue 5 (April 2008), pp. 7-9.
The Case of Victor Bout: Global Illicit Air Cargo Facilitator

Bout is believed to have been one of the world’s most prodigious arms traffickers, notorious for his ability to transport practically anything anywhere with his fleet of airplanes, primarily former Soviet cargo planes. Prior to his arrest and eventual conviction in 2011, Bout was widely believed to have had a hand in a range of international contraband smuggling and sanctions-busting activities in Africa, southwest Asia, and elsewhere. Both the United Nations and the U.S. government sought to freeze his assets, and Belgium issued an arrest warrant for him in 2002 for crimes related to money laundering and diamond smuggling. He has also been accused of illegally transporting arms to the Taliban and Al Qaeda, while legally providing air freight transport around the world, including under contract for the U.S. military in Iraq. He was caught in Thailand in 2008 in a DEA sting operation after attempting to sell surface-to-air missiles, AK-47s, ammunition, C-4 plastic explosives, and unmanned aerial vehicles to U.S. confidential sources purporting to be members of the FARC. Although Bout was ultimately extradited to the United States in November 2010, convicted in November 2011 on four counts, and sentenced to 25 years in prison in April 2012, other enterprising crime-terrorism facilitators may fill the vacuum he has left in the global illicit arms trade.

- **Corruption:** Through bribery, financial inducements, and other forms of coercion, including the credible threat of violence, both criminal and terrorist elements can take advantage of corrupt actors to facilitate their operations and reduce the likelihood of detection and capture. Corrupt actors may range from border guards, financial regulators, justice sector officials, high-level policymakers and political figures, to private bankers, small business owners, and industry magnates. Government protection may take several forms, such as selectively providing intelligence and other support to illicit actors; or the wholesale ceding of authority and legitimacy to an illicit group.

Organizational Evolution and Variation

Typically, criminal groups are primarily driven by profit motives, whereas terrorist groups are ideologically driven. The motivations that drive terrorist and criminal groups, however, can evolve with time. A purely criminal group may transform to adopt political goals and ideological motivations. Terrorist groups, on the other hand, may shift toward criminality. For some terrorist groups, criminal activity remains secondary to ideological ambitions. For others, profit-making may surpass political aspirations as the dominant operating rationale. The level of involvement and expertise in terrorist or criminal activities may vary, depending on the organization’s current leadership, membership composition, geographic distribution of sympathizers and diaspora networks, dependence on state sponsorship, and physical proximity or access to illicit resources.

Frequently cited terrorist organizations involved in criminal activity include, among others, ASG,

---


Al Qaeda’s affiliates, D-Company, PKK, FARC, Haqqani Network, and Hezbollah. Brief descriptions of these groups’ criminal activities are described below.

Abu Sayyaf Group (ASG)

A Philippines-based terrorist group, ASG appears to have at times prioritized criminal activities over ideological operations. Major shifts toward crime occurred in conjunction with leadership and membership composition changes, which altered the relative importance of ideological zeal and criminal tendencies. During its periods of high criminality, ASG became well known for its success in kidnappings for ransom, maritime piracy, and arms trafficking.\(^{67}\) Observers suggest that the group’s overall drive toward criminal activity has been perpetuated by the group’s ability to generate illicit profits, with new recruits tending to be more motivated by ASG’s promise of financial wealth rather than ideological convictions. The State Department has listed ASG as an FTO since 1997, and President George W. Bush designated ASG a specially designated global terrorist (SDGT) pursuant to EO 13224 in 2001.

Al Qaeda’s Affiliates

There is no conclusive evidence of senior-level Al Qaeda members directly involved with or motivated by organized crime. Many speculate that this is because of the group’s strict ideological beliefs and fear of a loss of credibility if senior leaders were found to be directly involved in such activities. Connections to organized crime activity, however, can be drawn among mid-level and low-level Al Qaeda members and supporters. Moreover, it appears that Al Qaeda’s affiliates and franchises do not necessarily share the same aversion to criminal activity. Notable crime-funded Al Qaeda affiliates include AQIM and AQI.\(^{68}\) Additionally, Al Qaeda’s disinclination toward direct involvement in organized crime has not prevented it from cooperating, supporting, and jointly training with other insurgent groups that are more entrenched in trafficking and smuggling activities, including the Haqqani Network and the Taliban. The State Department designated Al Qaeda as an FTO in October 1999, and President George W. Bush designated it as an SDGT pursuant to EO 13224 in 2001. Several of its affiliates have also been designated separately as FTOs, including AQI in December 2004, AQIM in February 2008 (AQIM was also previously designated in March 2002 when it was called the Salafist Group for Call and Combat, GSPC), and AQAP in January 2010.

---


The 2004 Madrid Bombing and Its Connections to Drugs

The Al Qaeda cell that committed the March 2004 train bombings in Madrid provides an example of terrorist cell whose members used extensive criminal endeavors to fund its operations. One of the plot’s ring leaders and several accomplices were drug dealers and traffickers before they became radicalized and joined the Madrid cell. These operatives sold narcotics to pay for cars, safe houses, phones, and other logistical support, and weapons. Furthermore, they reportedly exchanged drugs for the explosives used in the attacks. One of the masterminds of the Madrid bombings was reportedly Jamal Ahmidan, a major drug dealer who ran a far-reaching narcotics ring that sold hashish and Ecstasy throughout Western Europe in the 1990s. Ahmidan appears to have first become interested in extremist Islamic ideology while serving time in a Spanish prison in 1998, and then was fully radicalized in a Moroccan jail from 2000 to 2003.\(^\text{69}\)

D-Company

Dawood Ibrahim, the alleged leader of D-Company, is an INTERPOL fugitive and wanted in connection with the 1993 Mumbai bombing and sanctioned under U.N. Security Council Resolution 1267. Ibrahim was listed in October 2003 by the Treasury Department as a specially designated global terrorist (SDGT), and both Ibrahim and his organization were listed as significant foreign narcotics traffickers (SDNTKs) in May 2008, pursuant to the Foreign Narcotics Kingpin Designation Act. His organization, D-Company, can be characterized as both a transnational criminal syndicate as well as ideologically aligned with terrorist groups operating in South Asia, including Lashkar-e-Taiba (LeT). According to reports, D-Company originated as a smuggling operation in the 1970s. It evolved in the 1990s into an organized crime group not only motivated by profit but also one that engaged in insurgent activity, eventually supporting efforts to smuggle weapons to militant and terrorist groups in the region. By the 1990s, it began to conduct and participate in terrorist attacks, including the March 12, 1993, Bombay bombing. D-Company’s criminal activities reportedly span extortion, smuggling, narcotics trafficking, and contract killings.\(^\text{71}\) Its apparent willingness to work with and provide logistical, financial, and material support to ideologically motivated violent groups exemplifies the risks associated with converged criminal and terrorists threats.\(^\text{72}\)

Kurdistan Worker’s Party (PKK)

Formed in the 1970s and operational since the early 1980s as a Kurdish nationalist group with Marxist-Leninist leanings, the PKK increasingly turned to crime after it lost its state sponsors.\(^\text{73}\) By the late 1990s, and particularly after its leader Abdullah Ocalan was captured in 1999, the

---


\(^{72}\) Ben Riley and Kathleen Kiernan (Kiernan Group Holdings), eds., The ‘New’ Face of Transnational Criminal Organizations (TCOs): A Geopolitical Perspective and Implications to U.S. National Security, March 2013.

\(^{73}\) Its state sponsors included Syria, which hosted the group’s leadership, as well as the Soviet Union, Iran, Iraq, and Greece.
PKK invested heavily in transnational organized crime activities, such as drug trafficking, arms smuggling, human smuggling, extortion, money laundering, counterfeiting, and illegal cigarettes. By the 1990s, the PKK had formed specialized units to variously carry out militant operations, contraband trafficking, political activities, and information campaigns. As a result, some parts of the PKK appear to behave more like a criminal organization rather than a terrorist or guerrilla organization. According to the U.S. government, many of these criminal activities are centered in Europe, where there is a significant Kurdish diaspora population. The State Department designated the PKK as an FTO in October 1997. The PKK was also designated as an SDGT in 2001. For its alleged involvement in drug trafficking, the President designated the PKK as an SDNTK in May 2008, pursuant to the Foreign Narcotics Kingpin Designation Act.

Revolutionary Armed Forces of Colombia (FARC)

Operational since the 1960s, the FARC has been described as one of the largest, oldest, most violent, and best-equipped terrorist organization in Latin America. Its longevity is due in part to its involvement in the drug trade. The enormous profit opportunity that drug trafficking has provided to the FARC is widely viewed as the driving factor for its involvement in such criminal activity. According to reports, the FARC first became involved in the drug trade in the 1980s by levying protection fees on coca bush harvesters, buyers of coca paste and cocaine base, and cocaine processing laboratory operators in territory under FARC control. Over time, the FARC took a more direct role in drug production and distribution. By the 2000s, the FARC had reportedly become the world's largest supplier of cocaine. The FARC also reportedly generates revenue from extortion rackets, kidnapping ransoms, and illegal mining. Exploratory peace talks between the Colombian government and the FARC began in August 2012, the outcome of which may have implications for the FARC's future involvement in illicit criminal activities. The State Department designated the FARC as an FTO in October 1997.

Further CRS Reading

For more on the FARC, see CRS Report RS21049, Latin America: Terrorism Issues, by Mark P. Sullivan and June S. Beittel, and CRS Report RL32250, Colombia: Background, U.S. Relations, and Congressional Interest, by June S. Beittel.

---


75 Since the 2003 U.S.-led invasion of Iraq, the PKK has used safe havens in northern Iraq to coordinate and launch attacks against Turkish targets. PKK violence also appears to have resurfaced during the early stages of the “Arab Spring” and particularly following the outbreak of civil conflict in Syria. Some reports speculate that the Assad regime and Iran might be providing political and/or material support to these groups.

76 Rex A. Hudson et al., A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups, Library of Congress, Federal Research Division, May 2002; Eccarius-Kelly, “Surreptitious Lifelines ...,” 2012; U.S. Department of State, Country Reports on Terrorism 2011, July 2012. It is also believed to have entered into strategic alliances with external criminal syndicates and other terrorist organizations. The FARC, for example, reportedly maintains contacts with Russian, Ukrainian, Croatian, and Jordanian crime families, and armed groups in more than a dozen foreign countries, for the purposes of supplying the FARC with weapons and communications equipment. The FARC also allegedly collaborates with other terrorist groups, including Basque Homeland and Freedom (ETA) and a smaller insurgent group in Colombia, the National Liberation Army (ELN).
Haqqani Network

The family-run Haqqani Network is commonly described as an insurgent group, in equal measures one of the Taliban’s most capable militant factions as well as an enterprising transnational criminal organization. Headquartered in North Waziristan, Pakistan, this insurgent group is suspected of conducting major attacks against allied coalition members of the North Atlantic Treaty Organization (NATO) and U.S. forces in Afghanistan as well as active involvement in a wide range of highly profitable licit and illicit activity. In the 1980s, Jalaluddin Haqqani first gained a reputation as an effective mujahedin commander and U.S. ally against the Soviet Union. He later joined the Taliban regime in the 1990s when in power in Afghanistan. The group continues to maintain relationships not only with Al Qaeda and other militant groups in the region, but also purportedly benefits from a relationship with Pakistan’s Inter-Services Intelligence Directorate (ISI)—a relationship strongly decried by America’s top ranking military officer in September 2011. As part of a strategy of financial diversification to ensure the organization’s resiliency against external pressures, the group also benefits financially from extortion and protection rackets, robbery schemes, kidnapping for ransom, and contraband smuggling (e.g., drugs, precursor chemicals, timber, and chromite).77 The Haqqanis also reportedly control licit import-export, transportation, real estate, and construction firms through which illicit proceeds can be laundered. Pursuant to the Haqqani Network Terrorist Designation Act of 2012 (P.L. 112-168), the State Department designated the group as an FTO in September 2012.

Hezbollah

Based in Lebanon, with established cells in Africa, North and South America, Asia, and Europe, Hezbollah is known to have or suspected of having been involved in terrorist attacks against U.S. interests worldwide. Although primarily funded and trained with support from state sponsors, chiefly Iran, Hezbollah also reportedly benefits from a sprawling global commercial network of licit and illicit businesses, largely connected to expatriate Lebanese communities worldwide.78 Sources of funds include private donors and large-scale investments in legitimate businesses. Criminal indictments and statements by U.S. officials and other experts suggest that Hezbollah has also become well-integrated in the domain of transnational organized crime, deriving profits from a wide range of illicit enterprises, such as drug trafficking, precursor chemical trafficking, counterfeit

Further CRS Reading


Further CRS Reading

For more on Hezbollah, see CRS Report R41446, Hezbollah: Background and Issues for Congress, by Casey L. Addis and Christopher M. Blanchard.

---


pharmaceutical trafficking, sales of counterfeit commercial goods and electronics, auto theft and fraudulent re-sale, diamond smuggling, cigarette and baby formula smuggling, credit card fraud, and insurance scams, among potentially many others. Pursuant to EO 12947, Hezbollah was designated in January 1995 as a specially designated terrorist (SDT). The State Department designated Hezbollah as an FTO in 1997. In October 2001, Hezbollah was also designated as an SDGT pursuant to EO 13224.

Foreign Policy Responses

With recognition that every crime-terrorism partnering circumstance will be different and the tools to identify and address such concerns may change, a wide range of anti-crime and counterterrorism policy options can be considered. The variety of options available, however, also challenges policymakers to consider several key questions in formulating responses. Should a specific agency or an interagency coordinating body be designated as leading U.S. government responses to crime-terrorism threats? Under what circumstances would U.S. responses to crime-terrorism threats be most appropriately led by the intelligence community, military, diplomatic corps, or law enforcement agencies? How can resources and authorities be allocated and managed to avoid excessive duplication while also ensuring effective policy response coverage?

The following sections describe selected key foreign policy responses to crime-terrorism nexus threats and related policy considerations for Congress for each response. These may be applied in various combinations or sequences, depending on the specific circumstances.

Diplomacy

U.S. diplomatic efforts to promote anti-crime and counterterrorism goals occur through bilateral, regional, and multilateral mechanisms. Such efforts are often led by the U.S. Department of State and include initiatives developed by its regional bureaus, the Bureau for International Narcotics and Law Enforcement Affairs (INL), and the Bureau of Counterterrorism (CT). Relevant U.N. treaties to which the United States is party to include the International Convention Against the Taking of Hostages, International Convention for the Suppression of Terrorist Bombings, International Convention for the Suppression of the Financing of Terrorism, U.N. Convention against Transnational Organized Crime, and International Convention for the Suppression of Acts

of Nuclear Terrorism. Through the U.N. Security Council, the United States also participates in the Security Council Sanctions Committee. The Sanctions Committee administers and enforces a range of sanctions and targeted measures against Al Qaeda and the Taliban, among others, which include arms embargoes, travel bans, asset freezes, and diplomatic restrictions.

Bilaterally, the U.S. government maintains mutual legal assistance treaties (MLATs) and extradition agreements with foreign countries to facilitate transnational investigations and information sharing. Other options available to the State Department include designating entities as FTOs, pursuant to the Immigration and Nationality Act (INA), as amended, and barring known foreign terrorists and transnational organized criminals from entry into the United States and providing grounds to remove and deport such individuals if in the United States, pursuant to several visa ineligibility conditions.\textsuperscript{80} (See text box below for more on a recent FTO designation, the Haqqani Network.) Additionally, the U.S. Department of the Treasury’s Office of Terrorist Financing and Financial Crimes (TFFC) leads the U.S. delegation in meetings of the Financial Action Task Force (FATF), an international body that develops global regulatory standards for combating money laundering and terrorist financing.

Congress has provided direction to relevant federal departments to conduct diplomatic activities to address crime-terrorism issues by enacting legislation that authorizes and appropriates funds to relevant agencies to perform such tasks, as well as by conducting program oversight through hearings and reporting requirements. Given the inherently transnational nature of many current crime-terrorism challenges, diplomacy often plays a central role in responses. The extent to which diplomacy can be effective in combating crime-terrorism threats, however, is limited by delays associated with achieving consensus agreements and potentially long-lasting gaps in foreign political will and capacity.

Designating the Haqqani Network

As discussed above, the Haqqani Network is a militant faction of the Taliban, whose insurgent activities include acts of terrorism as well as extensive involvement in transnational criminal activity. Although several senior members of the group had previously been listed by the Treasury Department as SDGTs, the Haqqani Network was not designated as an FTO until September 2012. Congress contributed to its designation as an FTO with the passage of the Haqqani Network Terrorist Designation Act 2012 (S. 1959/H.R. 6036). Enacted on August 10, 2012 (P.L. 112-168), the act established that it was the sense of Congress that the Haqqani Network met the criteria for designation as an FTO pursuant to Section 219 of the Immigration and Nationality Act (INA) and that the Secretary of State should designate the group as such. The act required that the Secretary of State report to appropriate congressional committees within 30 days of enactment of the act with a detailed report on whether the Haqqani Network fit the description of FTOs. On September 7, 2012, the State Department transmitted its report to Congress, concluding that the Haqqani Network met the criteria for designation as an FTO; according to the State Department, it is a “foreign organization that engages in terrorism” and that its terrorist activity “threatens the security of U.S. nationals and the national security of the United States.”

Foreign Assistance

Several U.S. departments and agencies administer programs to train foreign law enforcement officials and other security forces; develop legal frameworks in partner nations to criminalize and combat various crime-, drug-, and terrorism-related activities; and support institutional capacity building for foreign internal security and border enforcement entities. U.S. foreign assistance efforts to combat international terrorism or transnational crime can have mutually beneficial implications. In cases of crime-terrorism confluence, some have cautioned that an increasingly blurred line between counterterrorism and anti-crime assistance could reduce foreign aid transparency and raise additional challenges in planning and coordinating projects to avoid redundancy. In some cases, foreign development aid may also risk unintentionally providing illicit groups with an additional source of funding. In regions where known crime-terrorist groups are known to operate, such as Afghanistan, funds intended for development projects have at times benefited illicit groups, who offer development contractors with security and protection services.81

Most U.S. foreign police assistance is administered through the U.S. Departments of State and Defense, and programs are variously implemented by other U.S. agencies and federal contractors in host nations. In some situations, the U.S. government may be requested to support foreign militaries in their efforts to combat crime-terrorism threats, such as the FARC in Colombia or the Taliban in Afghanistan. In addition to U.S.-funded foreign security forces support efforts, the U.S. Agency for International Development (USAID) is often involved in developing related justice sector and rule of law assistance programs. DOJ maintains in-house expertise through its Office of Overseas Prosecutorial Development Assistance and Training (OPDAT) and International Criminal Investigative Training Assistance Program (ICITAP) to implement capacity building projects that support foreign countries investigate and prosecute cases involving transnational crime and international terrorism. U.S. federal prosecutors may serve as Resident Legal Advisors (RLAs) overseas to support related justice sector training, institution building, and legislative drafting.

81 For one example in Afghanistan that may have resulted in development aid diverted to the Haqqani Network among other local militant groups, see Alissa J. Rubin and James Risen, “Costly Afghanistan Road Project is Marred by Unsavory Alliances,” The New York Times, May 1, 2011.
Congress has played an active role in establishing the scope and amount of U.S. assistance that can be provided for the purposes of counterterrorism and anti-crime. Specific authorities are outlined in the Foreign Assistance Act of 1961, as amended, Title 10 of the U.S. Code, and periodic National Defense Authorization Acts. Additional conditions may also be included in appropriations acts for the various agencies involved in administering foreign assistance for counterterrorism and anti-crime.

Financial Actions

Several unilateral and multilateral policy mechanisms are available to block transactions and freeze assets of specified terrorist or criminal entities, as well as to strengthen international financial systems through enhanced regulatory requirements. Unilaterally, the Treasury Department’s Office of Foreign Assets Control (OFAC) administers and enforces unilateral targeted financial sanctions against a list of foreign entities and individuals (specially designated nationals, or SDNs) that include SDGTs, FTPs, Middle Eastern terrorist organizations found to undermine and threaten Middle East peace process efforts (specially designated terrorists, or SDTs), transnational criminal organizations (TCOs), and specially designated narcotics traffickers and trafficking kingpins (SDNTs and SDNTKs). Authorities for OFAC to designate such entities are derived from executive order and legislative statutes, which include the International Emergency Economic Powers Act (EEPA), the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA), and the Foreign Narcotics Kingpin Designation Act.

Additionally, Title II of the USA PATRIOT ACT of 2001 (P.L. 108-56, as amended) introduced several policy tools that strengthened the existing U.S. framework to combat illicit finance. Among other provisions, this act developed a procedure, popularly known as Section 311, to apply enhanced regulatory requirements, called “special measures,” against designated jurisdictions, financial institutions, and international transactions that are found to be involved in criminal or terrorist financing activities. At the multilateral level, the United Nations administers several sanctions programs to freeze funds related to persons involved in acts of terrorism, including individuals and entities associated with Al Qaeda and the Taliban, pursuant to U.N. Security Council Resolution 1373 (2001), U.N. Security Council Resolution 1267 (1999), and U.N. Security Council Resolution 1988 (2011).

Many observers have argued that a key tool to combat the confluence of crime and terrorism is to follow their overlapping money trails and apply financial sanctions and heightened regulatory conditions to vulnerable financial sectors. Both types of groups require funds to sustain operations, and such funds often intersect with the formal international banking system. Critics of such tools to counter illicit financial transaction suggest that they are often laborious and time-intensive to implement, and not necessarily effective in dismantling crime or terrorism networks. Policymakers have acknowledged that criminals and terrorists continue to exploit opportunities to move funds and hide their financial tracks in multiple ways: in the formal financial system; through centuries-old techniques such as bulk cash smuggling, trade-based money laundering, and hawala-type informal value transfer systems; and through modern technologies such as prepaid cards, mobile banking systems, and the Internet.

---

82 Also highlighting the Treasury Department’s awareness in the aftermath of September 11 that both criminals and terrorists seek to exploit the international financial system, it established in 2004 the Office of Intelligence and Analysis (OIA), now a formal member of the intelligence community.
Intelligence

Although few details are publicly available about the intelligence community’s role in combating crime-terrorism threats, intelligence can play a significant role in developing strategic analyses that prioritize crime-terrorism trends of national security significance, as well as in developing operational and tactical responses to detect, influence, and target specific crime-terrorism networks, nodes, plans, and actors. The 2009 National Intelligence Strategy described the nexus between terrorism and criminal activities as among the intelligence community’s priorities.

In the past, some have suggested that there appeared to be limited, if any, systematic gathering of intelligence related to the nexus between crime and terrorism and, as a result, an incomplete understanding of the scope and nature of relationships between and convergence among terrorists and criminal actors. The Obama Administration’s 2011 Strategy to Combat Transnational Organized Crime acknowledged that “a shift in U.S. intelligence collection priorities” since 9/11 resulted in “significant gaps” related to transnational organized crime.\(^3\) The 2011 Strategy also identified the enhancement of “U.S. intelligence collection, analysis, and counterintelligence” on transnational organized crime as “a necessary first step.” Since 9/11, numerous bills have addressed terrorism as well a transnational crime-related issues. Similarly, a number of congressional hearings have focused on issues relating to international terrorism and transnational crime. Some observers suggest that heightened congressional focus on the confluence of crime and terrorism may have an impact on the executive branch’s approach to the issue and appreciation for the risks and vulnerabilities associated with crime-terrorism partnering arrangements.

Military Actions

In some cases, particularly in non-permissive security environments in which traditional law enforcement units may have difficulty operating, the U.S. military has been called upon to contribute to certain joint counternarcotics and counterterrorism or counterinsurgency activities. In 2002, for example, Congress first authorized DOD to support a “unified campaign against narcotics trafficking ... [and] activities by organizations designated as terrorist organizations such as the Revolutionary Armed Forces of Colombia (FARC), the National Liberation Army (ELN), and the United Self-Defense Forces of Colombia (AUC).\(^4\) Although Congress renewed this authority through FY2012 in the National Defense Authorization Act for Fiscal Year 2012 (P.L. 112-81), it has not been codified and is limited only to activities in Colombia. Military operations in Afghanistan provide another example in which DOD has taken an expanded approach to crime-terrorism nexus issues. In late 2008, DOD amended its rules of engagement in Afghanistan to allow U.S. military commanders to target drug traffickers and others who provide material support to insurgent or terrorist groups such as the Taliban and members of hybrid crime-terrorism groups such as the Haqqani Network.\(^5\) DOD further clarified that the U.S. military may accompany and provide force protection in counternarcotics field operations.\(^6\) In some cases, the

---


\(^4\) Section 305 of P.L. 107-206.


U.S. military has chosen to take lethal action to rescue or attempt to rescue hostages in kidnapping for ransom situations.\textsuperscript{87}

U.S. military involvement in situations where there are overlaps between anti-crime and counterterrorism goals is not necessarily warranted or desired. In some situations, political sensitivities and rules of engagement may prevent or prohibit the U.S. Armed Forces from direct involvement. Some observers caution that militarized counternarcotics or anti-crime policies may risk escalating suppression tactics and contribute to violations of human rights.

**Investigations**

Various elements of the U.S. Departments of Justice (DOJ) and the Department of Homeland Security (DHS) are tasked with investigating cases that involve alleged prohibited acts related to international terrorism and transnational crime. These include the U.S. Federal Bureau of Investigation (FBI), the U.S. Drug Enforcement Administration (DEA), the International Organized Crime Intelligence and Operations Center (IOC-2), and Immigration and Customs Enforcement (ICE). The State Department, DOD, and FBI also publicize rewards programs for citizen tips that lead to the apprehension of selected high-profile perpetrators of transnational organized crime, including money launderers, human traffickers, and drug traffickers, as well as terrorists.\textsuperscript{88}

Some observers see the nexus between crime and terrorism as a potential benefit for detection and law enforcement prosecution that could be further exploited. Even if prosecutors do not have sufficient evidence to convict a suspected terrorist of terrorism-related charges, other criminal charges may be effectively used. Furthermore, some criminal charges, such as violations related to drug trafficking, can lead to jail sentences and penalties similar in magnitude to terrorism ones. It remains unclear, however, how effective such law enforcement and prosecution approaches have been to combat terrorism or how frequently such strategies have been implemented in practice, both in the United States and among partner nations, due to the lack of consistency in tracking cases with crime-terrorism nexus connections. Congress may have an interest in assessing how existing statutes have been used to support investigative and prosecution-related activities in response to entities suspected of engaging in terrorism-crime partnering activities. Assessing investigative, prosecution, and sentencing data collected in the 11 years since the attacks of 9/11 may provide Congress with information regarding statutes that have been effectively used to address crime-terrorism partnering activities and areas where additional legislative assistance might be required.


\textsuperscript{88} In early January 2013, the 112th Congress enacted the Department of State Rewards Program Update and Technical Corrections Act of 2012 (P.L. 112-283). Prior to its enactment, the State Department’s rewards programs were limited to offering payments for information leading to the arrest or conviction of individuals involved in major narcotics trafficking or international terrorism.
Investigation and Enforcement of International Narcoterrorism Cases

Section 122 of the USA PATRIOT Improvement and Reauthorization Act of 2005 (P.L. 109-177) added a new prohibition against narco-terrorism with enhanced criminal penalties. This provision, codified at 21 U.S.C. 960a, makes it a violation of U.S. law to engage in narcotics-related crimes anywhere in the world while knowing, conspiring, or intending to provide support, directly or indirectly, for a terrorist act or to a terrorist organization. In order to pursue these complex, transnational narco-terrorism cases against high-level, often foreign or foreign-located targets, DEA established the Counter-Narco-Terrorism Operations Center within its Special Operations Division (SOD) to manage its worldwide activities. In some countries, such as in Afghanistan, narco-terrorism operations are implemented on the ground through Foreign-Deployed Advisory and Support Teams (FAST) that collaborate on joint investigations together with host country counterparts.

There have been several publicly reported investigations and prosecutions involving alleged violations of 21 U.S.C. 960a. Such cases have involved individuals allegedly affiliated with groups, such as the Taliban, the United Self-Defense Forces of Colombia (AUC), Al Qaeda, Hezbollah, and the FARC.

International narco-terrorism prosecutions appear to have gained prominence since enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005. For example, the Office of the U.S. Attorney for the Southern District of New York internally restructured its organizational units in January 2010 and merged its Terrorism and National Security Unit with its International Narcotics Trafficking Unit. This internal reorganization was designed to facilitate greater coordination with DEA on narco-terrorism cases. Explaining the apparent increased emphasis on narco-terrorism, the U.S. Attorney for the Southern District of New York stated:

Since January 2010, this Office, in partnership with the DEA, has focused its attention even more closely on the serious threat that narco-terrorism poses to our national security. Combating the lethal nexus of drug trafficking and terrorism requires a bold and proactive approach. And as crime increasingly goes global, and national security threats remain global, the long arm of the law has to get even longer.  

Meanwhile, some observers have raised questions about the implementation of 21 U.S.C. 960a and related statutes in practice. Some have questioned whether the U.S. government approach to investigating and, ultimately, prosecuting individuals under 21 U.S.C. 960a sufficiently targets the most significant foreign drug and terrorism threats to U.S. interests. Others question whether pursuit of foreign narco-terrorism suspects overseas and subsequent prosecution in U.S. courts is the most appropriate policy tool choice.

Looking Ahead: Implications for Congress

Policy issues related to the interaction of international crime and terrorism are inherently complex. While the U.S. government has maintained substantial long-standing efforts to combat terrorism and transnational crime separately, questions remain about how and whether issues related to the interaction of the two threats are handled most effectively across the multiple U.S. agencies involved. Efforts to combat transnational crime can result in positive and negative outcomes with counterterrorism policies, raising fundamental questions about how to prioritize combating crime or terrorism aspects of a case when both elements are present. Further, questions remain on how links between terrorist-criminal activity and potentially related U.S. polices—


including but not limited to WMD proliferation, cyber security, post-conflict reconstruction efforts, and counterinsurgency—are integrated across agencies.

Since the September 11 attacks, Congress has enacted several landmark bills that have given the U.S. government greater authority and additional tools to counter the convergence of organized crime and terrorism. Less than six weeks after the attack, Congress enacted the USA PATRIOT Act (P.L. 107-56) to strengthen the U.S. government's ability to detect, report, and prevent terrorist activities, including potential connections between organized crime and terrorism. Additionally, Congress enacted the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) and the USA PATRIOT Improvement and Reauthorization Act of 2005 (P.L. 109-177), which further enhanced U.S. government efforts to crack down on terrorist financing and money laundering.

Based on recent U.S. assessments, transnational crime and international terrorism appear to intersect and overlap in ways that will, at times, affect U.S. national interests. To this end, Congress may choose to continue to evaluate existing approaches and programs to combat the confluence of crime and terrorism through hearings and requesting or legislating reports to be issued by relevant executive branch agencies and inspector general offices. Congress may also choose to modify, adapt, or enhance existing legislative authorities and mandates to target various dimensions of the problem. Such approaches may be region- or group-specific, or global in scope.

More broadly, as policymakers consider the crime-terrorism nexus issue and relevant policy responses, key questions for Congress may include the following:

- What is the scope of the crime-terrorism issue? What types of crimes are involved? Which groups and actors of both kinds pose the greatest threat to U.S. national security?

- What political, social, economic, geographic, and demographic circumstances facilitate the interaction between transnational crime and international terrorism?

- Has the United States successfully exploited the partnering arrangements and differences in motivations and capabilities of terrorist groups and criminal organizations? If so, what lessons learned could apply to current and future activities by such actors?

- What prevents the U.S. government and international community from disrupting and dismantling current crime-terrorism threats?

---

91 The PATRIOT Act, for example, stiffened money laundering penalties, granted the Secretary of the Treasury new powers, established mechanisms to report money laundering transactions through private banks, permitted the transfer of financial records among agencies if relevant to intelligence activities, created Federal jurisdiction over foreign money launderers, and made licensed money senders, including informal hawala networks, subject to mandatory reports on transactions.

92 Among other provisions, the Intelligence Reform and Terrorism Prevention Act of 2004 expanded the authority and tools of the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), directed the Secretary of the Treasury to prescribe regulations requiring financial institutions to report certain cross-border money transfers, and directed the president to submit to Congress a report evaluating U.S. efforts to curtail international financing of terrorism. Pertaining to potential crime-terrorism connections, the USA PATRIOT Improvement and Reauthorization Act of 2005 increased penalties for terrorism financing, expanded the purview of the Racketeer Influenced and Corrupt Organizations (RICO) Act (P.L. 91-452), broadened the parameters of money laundering offenses, and made the receipt of military training from a foreign terrorist organization a predicate to a money laundering offense.
• Which federal government entities have the lead roles for addressing various aspects of the crime-terrorism phenomenon?

• How are government funds being spent to address concerns about crime-terrorism links?

• Is there a need to expand or adjust existing congressional authorities to combat the combined crime-terrorism threat? Are the available U.S. foreign policy tools sufficient to meet today’s crime-terrorism concerns—and are such tools effectively implemented? If not, what can be improved?
Appendix. Terrorist Links to Criminal Financing

The following table summarizes the State Department’s descriptions of how current foreign terrorist organizations (FTOs) raise funds and whether, if at all, an FTO is involved in criminal activities as a source of revenue. Among the 51 FTOs described in the State Department’s most recent Country Reports on Terrorism (from May 2013), sources of funding vary. Common sources of funding include, in various combination, state sponsors, private donors, other terrorist groups, legitimate business activity, proceeds of crime. Popular forms criminal financing include extortion, kidnapping for ransom, drug trafficking, robbery, human smuggling, weapons smuggling, other contraband smuggling, money laundering, bank fraud, credit card fraud, cybercrime, immigration fraud, passport falsification, and illegal charcoal production. For 9 of the 51 FTOs, the State Department reports that funding sources and mechanisms are “unknown.”

Table A-1. Foreign Terrorist Organization (FTOs): Reported Sources of External Aid

<table>
<thead>
<tr>
<th>Foreign Terrorist Organization</th>
<th>Abbreviation</th>
<th>Designation Date</th>
<th>Criminal Financing?</th>
<th>Additional Description of Sources of Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revolutionary Organization 17 November</td>
<td>17N</td>
<td>October 8, 1997</td>
<td></td>
<td>Funding and external aid are “unknown.”</td>
</tr>
<tr>
<td>Asbat al-Ansar</td>
<td>AAA</td>
<td>March 27, 2002</td>
<td></td>
<td>“It is likely that the group receives money through international Sunni extremist networks.”</td>
</tr>
<tr>
<td>Abdullah Azzam Brigades</td>
<td>AAB</td>
<td>May 30, 2012</td>
<td></td>
<td>Funding and external aid are “unknown.”</td>
</tr>
<tr>
<td>Al-Aqsa Martyrs Brigade</td>
<td>AAMB</td>
<td>March 27, 2002</td>
<td></td>
<td>“Iran has exploited AAMB's lack of resources and formal leadership by providing funds and guidance, mostly through Hizballah facilitators.”</td>
</tr>
<tr>
<td>Ansar Al-Islam</td>
<td>Al</td>
<td>March 22, 2004</td>
<td></td>
<td>“Al receives assistance from a loose network of associates in Europe and the Middle East.”</td>
</tr>
<tr>
<td>Al-Shabaab</td>
<td></td>
<td>March 18, 2008</td>
<td>Yes</td>
<td>“Al-Shabaab continued to have sufficient financing available.... ” Sources include “funds from illegal charcoal production and exports from smaller ports along the coast, taxation of local populations and areas under al-Shabaab control, and foreign donations.” It also receives “significant donations from the global Somali diaspora....”</td>
</tr>
<tr>
<td>Abu Nidal Organization</td>
<td>ANO</td>
<td>October 8, 1997</td>
<td></td>
<td>“The ANO’s current access to resources is unclear, but it is likely that the decline in support previously provided by Libya, Syria, and Iran has had a severe impact on its capabilities.”</td>
</tr>
<tr>
<td>Army of Islam</td>
<td>AOI</td>
<td>May 19, 2011</td>
<td>Yes</td>
<td>“AOI receives the bulk of its funding from a variety of criminal activities in Gaza.”</td>
</tr>
<tr>
<td>Foreign Terrorist Organization</td>
<td>Abbreviation</td>
<td>Designation Date</td>
<td>Criminal Financing?</td>
<td>Additional Description of Sources of Support</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Al-Qa’ida</td>
<td>AQ</td>
<td>October 8, 1999</td>
<td>Yes</td>
<td>“AQ primarily depends on donations from like-minded supporters as well as from individuals who believe that their money is supporting a humanitarian cause. Some funds are diverted from Islamic charitable organizations.” Additionally, as previous opportunities “for receiving and sending funds have become more difficult to access, several affiliates have engaged in kidnapping for ransom. Through kidnapping for ransom operations and other criminal activities, the affiliates have also increased their financial independence.” AQ and Hizballah sympathizers located in South America and the Caribbean “continued to provide financial and ideological support ....”</td>
</tr>
<tr>
<td>Al-Qa’ida in the Arabian Peninsula</td>
<td>AQAP</td>
<td>January 10, 2010</td>
<td>Yes</td>
<td>“AQAP’s funding primarily comes from robberies and kidnap for ransom operations and to a lesser degree from donations from like-minded supporters.”</td>
</tr>
<tr>
<td>Al-Qa’ida in Iraq</td>
<td>AQI</td>
<td>December 17, 2004 (amended December 11, 2011)</td>
<td>Yes</td>
<td>“AQI receives most of its funding from a variety of businesses and criminal activities within Iraq.”</td>
</tr>
<tr>
<td>Al-Qa’ida in the Islamic Maghreb (formerly the Salafist Group for Call and Combat)</td>
<td>AQIM (formerly GSPC)</td>
<td>March 27, 2002 (amended February 20, 2008)</td>
<td>Yes</td>
<td>“AQIM members engaged in kidnapping for ransom and criminal activities to finance their operations.” Kidnapping operations, which typically targeted those with an “established pattern of making concessions in the form of ransom payments ...”, reportedly “continued to yield significant sums for AQIM...” Additionally, “Algerian expatriates and AQIM supporters abroad – many residing in Western Europe – may also provide limited financial and logistical support.”</td>
</tr>
<tr>
<td>Abu Sayyaf Group</td>
<td>ASG</td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>“The ASG is funded through kidnapping for ransom operations and extortion, and many also receive funding from external sources such as remittances from overseas Philipines workers and Middle East-based violent extremists. In the past, the ASG has also received assistance from regional terrorist groups such as Jemaah Islamiya, whose operatives provided training to ASG members and helped facilitate several ASG terrorist attacks.”</td>
</tr>
<tr>
<td>United Self-Defense Forces of Colombia</td>
<td>AUC</td>
<td>September 10, 2001</td>
<td>Yes</td>
<td>“As much as 70 percent of the AUC’s paramilitary operations costs were financed with drug-related earnings. Some former members of the AUC never demobilized or are recidivists, and these elements have continued to engage heavily in criminal activities.”</td>
</tr>
<tr>
<td>Aum Shinrikyo</td>
<td>AUM</td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>“Funding primarily comes from member contributions.”</td>
</tr>
<tr>
<td>Continuity Irish Republican Army</td>
<td>CIRA</td>
<td>July 13, 2004</td>
<td>Yes</td>
<td>“CIRA supported its activities through criminal activities, including smuggling.” The group carries out “bombings, assassinations, kidnappings, hijackings, extortion, and robberies.”</td>
</tr>
<tr>
<td>Communist Party of the Philippines / New People’s Army</td>
<td>CPP/NPP</td>
<td>August 9, 2002</td>
<td>Yes</td>
<td>“The CPP/NPA raises funds through extortion.”</td>
</tr>
<tr>
<td>Foreign Terrorist Organization</td>
<td>Abbreviation</td>
<td>Designation Date</td>
<td>Criminal Financing</td>
<td>Additional Description of Sources of Support</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Revolutionary People's Liberation Party/Front</td>
<td>DHKP/C</td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>&quot;The DHKP/C finances its activities chiefly through donations and extortion and raises funds primarily in Europe.&quot;</td>
</tr>
<tr>
<td>Revolutionary Struggle</td>
<td>EA</td>
<td>May 18, 2009</td>
<td></td>
<td>Funding and external aid are &quot;unknown.&quot;</td>
</tr>
<tr>
<td>National Liberation Army</td>
<td>ELN</td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>&quot;The ELN draws its funding from the narcotics trade and from extortion of oil and gas companies. Additional funds are derived from kidnapping ransoms. There is no known external aid.&quot;</td>
</tr>
<tr>
<td>Basque Fatherland and Liberty</td>
<td>ETA</td>
<td>October 8, 1997</td>
<td></td>
<td>&quot;ETA is probably experiencing financial shortages given that the group announced publicly in September 2011 that it had ceased collecting ‘revolutionary taxes’ from Basque businesses. This extortion program was a major source of ETA’s income.&quot;</td>
</tr>
<tr>
<td>Revolutionary Armed Forces of Colombia</td>
<td>FARC</td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>&quot;Today, it only nominally fights in support of Marxist goals, and is heavily involved in narcotics production and trafficking. The FARC has well-documented ties to the full range of narcotics trafficking activities, including extortion, cultivation, and distribution.&quot; Some human smuggling in the Darien Region of Panama was &quot;facilitated by FARC elements operating on both sides of the border.&quot;</td>
</tr>
<tr>
<td>Moroccan Islamic Combatant Group</td>
<td>GICM</td>
<td>October 11, 2005</td>
<td>Yes</td>
<td>&quot;In the past, GICM has been involved in narcotics trafficking in North Africa and Europe to fund its operations.&quot;</td>
</tr>
<tr>
<td>Hamas</td>
<td></td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>&quot;Hamas receives funding, weapons, and training from Iran. In addition, the group raises funds in the Persian Gulf countries and receives donations from Palestinian expatriates around the world, through its charities, such as the umbrella fundraising organization, the Union of Good. Some fundraising and propaganda activity also takes place in Western Europe.&quot; Hamas, among others, &quot;smuggled weapons, cash, and other contraband into Gaza through an extensive network of tunnels from Egypt.&quot; The group is also known to &quot;retain a cadre of leaders and facilitators that conduct political, fundraising, and arms-smuggling activities throughout the region.&quot;</td>
</tr>
</tbody>
</table>
| Hizbollah                                     |              | October 8, 1997  | Yes                | "Iran continues to provide Hizbollah with training, weapons, and explosives, as well as political, diplomatic, monetary, and organizational aid; Syria furnished training, weapons, diplomatic, and political support. Hizbollah also receives funding from private donations and profits from legal and illegal businesses. Hizbollah receives financial support from Lebanese Shia communities in Europe, Africa, South America, North America, and Asia. As illustrated by the Lebanese Canadian bank case, Hizbollah supporters are often engaged in a range of criminal activities that benefit the group financially. These have included smuggling contraband goods, passport falsification, trafficking in narcotics, money laundering, and credit card, immigration, and bank fraud." AQ and Hizbollah sympathizers located South American and Caribbean "continued to provide financial and ideological support...."
<table>
<thead>
<tr>
<th>Foreign Terrorist Organization</th>
<th>Abbreviation</th>
<th>Designation Date</th>
<th>Criminal Financing?</th>
<th>Additional Description of Sources of Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Haqqani Network</td>
<td>HQN</td>
<td>September 19, 2012</td>
<td>Yes</td>
<td>HQN draws strength through cooperation with other terrorist organizations operating in Afghanistan, including the Afghan Taliban, al-Qa'ida, Tehrik-e Taliban Pakistan, the Islamic Movement of Uzbekistan, Lashkar-e Jhangvi, and Jaish-e-Mohammad. In addition to such cooperative support, “HQN receives much of its funds from donors in Pakistan and the Gulf, as well as through criminal activities such as kidnappings, extortion, smuggling, and other licit and illicit business ventures.”</td>
</tr>
<tr>
<td>Harakat-ul Jihad Islami</td>
<td>HUJI</td>
<td>August 6, 2010</td>
<td></td>
<td>Funding and external aid are “unknown.”</td>
</tr>
<tr>
<td>Harakat ul-Jihad-i-Islami/Bangladesh</td>
<td>HUJI-B</td>
<td>March 5, 2008</td>
<td></td>
<td>“HUJI-B funding comes from a variety of sources. Several international Muslim NGOs may have funneled money to HUJI-B and other Bangladeshi militant groups.”</td>
</tr>
<tr>
<td>Harakat ul-Hujahideen</td>
<td>HUM</td>
<td>October 8, 1997</td>
<td></td>
<td>“HUM collects donations from wealthy and grassroots donors in Pakistan. HUM’s financial collection methods include soliciting donations in magazine advertisements and pamphlets.”</td>
</tr>
<tr>
<td>Gama’s Al-Islamiyya</td>
<td>IG</td>
<td>October 8, 1997</td>
<td></td>
<td>Funding and external aid are “unknown.”</td>
</tr>
<tr>
<td>Islamic Jihad Union</td>
<td>IJU</td>
<td>June 17, 2005</td>
<td></td>
<td>Funding and external aid are “unknown.”</td>
</tr>
<tr>
<td>Islamic Movement of Uzbekistan</td>
<td>IMU</td>
<td>September 20, 2000</td>
<td></td>
<td>“The IMU receives support from a large Uzbek diaspora, terrorist organizations, and donors from Europe, Central and South Asia, and the Middle East.”</td>
</tr>
<tr>
<td>Indian Mujahideen</td>
<td>IM</td>
<td>September 19, 2011</td>
<td></td>
<td>“Suspected to obtain funding and support from other terrorist organizations, such as LeT and HUJI, and from sources in Pakistan and the Middle East.”</td>
</tr>
<tr>
<td>Jemaah Ansharut Tauhid</td>
<td>JAT</td>
<td>March 13, 2012</td>
<td>Yes</td>
<td>“JAT raises funds through membership donations, as well as bank robberies, cyber hacking, and other illicit activities; and legitimate business activities such as operating bookstores and other shops.” Bank robberies and other illicit activities are carried out “to fund the purchase of assault weapons, ammunition, explosives, and bomb-making materials.”</td>
</tr>
<tr>
<td>Jaish-e-Mohammed</td>
<td>JEM</td>
<td>December 26, 2001</td>
<td></td>
<td>JEM “collects funds through donation requests in magazines and pamphlets, sometimes using charitable causes to solicit donations.” Since 2007, “JEM has withdrawn funds from bank accounts and invested in legal businesses, such as commodity trading, real estate, and production of consumer goods.”</td>
</tr>
<tr>
<td>Jemaah Islamiya</td>
<td>JI</td>
<td>October 23, 2002</td>
<td>Yes</td>
<td>“Investigations have indicated that JI is fully capable of its own fundraising through membership donations and criminal and business activities. It has received financial, ideological, and logistical support from Middle Eastern contacts and NGOs.”</td>
</tr>
<tr>
<td>Jundallah</td>
<td></td>
<td>November 4, 2010</td>
<td></td>
<td>Funding and external aid are “unknown.”</td>
</tr>
<tr>
<td>Kahane Chai</td>
<td></td>
<td>October 8, 1997</td>
<td></td>
<td>“Received support from sympathizers in the United States and Europe.”</td>
</tr>
<tr>
<td>Kata‘ib Hizballah</td>
<td>KH</td>
<td>July 2, 2009</td>
<td></td>
<td>“KH is almost entirely dependent on support from Iran and Lebanese Hizballah.”</td>
</tr>
<tr>
<td>Foreign Terrorist Organization</td>
<td>Abbreviation</td>
<td>Designation Date</td>
<td>Criminal Financing</td>
<td>Additional Description of Sources of Support</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Lashkar-e-Tayyiba</td>
<td>LeT</td>
<td>December 26, 2001</td>
<td></td>
<td>“LeT collects donations in Pakistan and the Gulf as well as from other donors in the Middle East and Europe, particularly the UK.” Funding and external aid are “unknown.”</td>
</tr>
<tr>
<td>Libyan Islamic Fighting Group</td>
<td>LIG</td>
<td>December 17, 2004</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lashkar I Jhangvi</td>
<td>Lj</td>
<td>January 30, 2003</td>
<td>Yes</td>
<td>“Funding comes from wealthy donors in Pakistan, as well as the Middle East, particularly Saudi Arabia. The group engages in criminal activity to fund its activities, including extortion and protection money.”</td>
</tr>
<tr>
<td>Liberation Tigers of Tamil Eelam</td>
<td>LTTE</td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>“The LTTE used its international contacts and the large Tamil diaspora in North America, Europe, and Asia to procure weapons, communications, funding, and other needed supplies. The group employed charities as fronts to collect and divert funds for their activities.” The group’s “financial network of support continued to operate throughout 2012, and there were multiple reports of increased LTTE involvement in human smuggling out of refugee camps.”</td>
</tr>
<tr>
<td>Popular Front for the Liberation of Palestine</td>
<td>PFLP</td>
<td>October 8, 1997</td>
<td></td>
<td>“Leadership received safe haven in Syria.”</td>
</tr>
<tr>
<td>Popular Front for the Liberation of Palestine-General Command</td>
<td>PFLP-GC</td>
<td>October 8, 1997</td>
<td></td>
<td>“The group’s primary recent focus was supporting Hizballah’s attacks against Israel, training members of other Palestinian terrorist groups, and smuggling weapons.” PFLP-GC received “safe haven and logistical and military support from Syria and financial support from Iran.”</td>
</tr>
<tr>
<td>Palestine Islamic Jihad—Shaqaqi Faction</td>
<td>PJ</td>
<td>October 8, 1997</td>
<td></td>
<td>“Receives financial assistance and training primarily from Iran.”</td>
</tr>
<tr>
<td>Kurdistan Workers’ Party</td>
<td>PKK</td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>“The PKK receives financial support from the large Kurdish diaspora in Europe and from criminal activity.” Funding and external aid are “unknown.”</td>
</tr>
<tr>
<td>Palestine Liberation Front—Abbas Faction</td>
<td>PLF</td>
<td>October 8, 1997</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real IRA</td>
<td>RIRA</td>
<td>May 16, 2001</td>
<td></td>
<td>“The RIRA is suspected of receiving funds from sympathizers in the United States and of attempting to buy weapons from U.S. gun dealers. The RIRA was also reported to have purchased sophisticated weapons from the Balkans and to have occasionally collaborated with the Continuity Irish Republican Army.”</td>
</tr>
<tr>
<td>Shining Path</td>
<td>SL</td>
<td>October 8, 1997</td>
<td>Yes</td>
<td>“SL is primarily funded by the narcotics trade.”</td>
</tr>
<tr>
<td>Tehrik-e Taliban Pakistan</td>
<td>TTP</td>
<td>September 1, 2010</td>
<td>Yes</td>
<td>“TTP is believed to raise most of its funds through kidnapping for ransom and operations that target Afghanistan-bound military transport trucks for robbery. Such operations allow TTP to steal military equipment, which it sells in Afghan and Pakistani markets.”</td>
</tr>
</tbody>
</table>

Author Contact Information

John Rollins  
Specialist in Terrorism and National Security  
jrollins@crs.loc.gov, 7-5529  

Liana Sun Wyler  
Analyst in International Crime and Narcotics  
lwyler@crs.loc.gov, 7-6177  

Acknowledgments

Updates to this report continue to benefit from the substantive contributions provided by Seth Rosen, former research associate at CRS in 2009.
PANEL V:

CYBERSECURITY: FUTURE CHALLENGES

MODERATOR:
MARY DE ROSA
Targeted attacks are inevitable in organizations with sensitive data. Depending on the situation, a targeted attack may involve the theft of source code, negotiation data, or general business disruption. Companies need to be prepared to identify, respond, and mitigate a targeted attack with the same amount of effort that goes into implementing a disaster recovery plan. From decades of experience, the consultants at CrowdStrike have created the following checklists to help organizations prepare for and respond to targeted attacks.

BEFORE A TARGETED ATTACK:

- **Consolidate and Monitor Internet Egress Points:** All connections to the internet from your corporate environment should be monitored to identify which information is leaving the environment. The less egress points to monitor, the easier it is to detect potentially malicious activity.

- **Leverage Host Based Detection:** As the workforce becomes more mobile, centralized network intrusion detection systems are not always in a position to inspect network traffic from a mobile workforce. Computers should utilize software similar to the CrowdStrike Falcon platform, to detect tactics, techniques, and procedures from targeted attackers.

- **Implement a Tiered Active Directory Administration Model:** CrowdStrike recommends using at least three levels of administration to isolate credentials and prevent the compromise of critical credentials. These levels are Domain Admins, Server Admins, and Workstation Admins. No single account can access all systems. There are several ways to accomplish this depending upon your environment.

- **Minimize or Remove Local Administrative Privileges:** Users should not utilize accounts with Local Administrator privileges as this creates multiple ways for targeted attackers to move laterally and compromise credentials. CrowdStrike recommends disabling the Local Administrator Account in an Active Directory Domain, the Local Administrator on workstations and servers should be disabled.

- **Implement Centralized and Time-Synchronized Logging:** DHCP, DNS, Active Directory, Server Event Logs, Firewall Logs, IDS, and Proxy Logs should all be stored in a protected centralized system that is time synchronized and easily searchable.

- **Have an Incident Response Services Retainer in Place:** Evaluate Incident Response firms in advance of when you may need their services, so that you have a plan in place if a targeted attack occurs.

- **Identify, Isolate, and Log Access to Critical Data:** Determine where your most sensitive data is located and implement logging and monitoring of access to it - NOW!

- **Patch, Patch, and Patch:** Patching operating systems and third party applications is one of the best ways to harden a network against a targeted attack. Critical security patches should be installed as soon as possible.

- **Subscribe to Cyber Intelligence Feeds:** Obtaining an understanding of who may be targeting you and the tactics they will likely use can help you to prioritize detection capabilities that will protect your sensitive data.

- **Review Reporting Requirements:** Identify which organizations and customers you have a responsibility to notify in the event of a security breach, and prepare documents and perform a legal review in advance.

RESPONDING TO A TARGETED ATTACK:

- **DO NOT DISCONNECT:** The majority of Targeted Attacks go on for months to years before being detected. When a compromised system is hastily disconnected, it is highly probable that the attacker will compromise additional systems to establish other forms of persistence that may go undetected. If a computer must be disconnected, ensure that a forensic image (to include a memory image) of the system is preserved prior to disconnecting power.

- **Preserve ALL Logs:** Validate that all centralized host-based and network-based logs are being preserved and that backups of critical servers are being maintained.

- **Establish Out-of-Band Communication Channels:** Assume that your network is completely compromised and the attacker can read email messages.

- **Contact an Incident Response Services Company:** This should be a company you already established a retainer with in the previous checklist.

- **Scope the Incident:** Conduct Network Forensics; Conduct Host Forensics to determine how many systems have been accessed or compromised and which data may have been accessed.

- **Remediate the Attack:** Isolate Critical Systems; Block access to Command and Control Infrastructure; Remove and replace infected hosts; Perform Credential Resets where needed; Assess additional measures to harden the environment.

- **Report:** Deliver required reporting per requirements and determine if media reporting is necessary.

Each environment is unique and will require additional items depending on the goals of the organization as well as the types of attacks that may be leveraged. CrowdStrike is available to help your organization prepare for a targeted attack, or to investigate one when it occurs.

Contact: Steven R. Chabinsky
General Counsel & Chief Risk Officer
Chabinsky@CrowdStrike.com
202.870.1442
Cybersecurity Strategy: A Primer
for Policy Makers and Those on the Front Line

Steven R. Chabinsky*

THE PROBLEM

The Internet seems to offer the promise of everything to everyone. For
global and local business, it lowers costs while increasing innovation,
invention, effectiveness, and efficiencies. For wealthy and poor economies
alike, the Internet greatly expands markets for products and services. For
peoples free and repressed, it provides an inlet and an outlet of expression.
For large and small communities, whether living in urban centers or
outlying regions, the Internet enables control over critical power,
transportation, water, and sewerage systems.

Lest we forget, for sophisticated criminals, terrorists, warmongers, and
spies, the Internet also offers the chance of a lifetime to cheat, steal, and
strike from afar with little money, covered tracks, and enormous real world
impact. While the ability to use the same technology for positive or
destructive ends is neither new nor momentous, it is necessary to consider
whether the rapid adoption of the Internet has provided so considerable an
asymmetric advantage to our adversaries that it can change the course of
American history. In this regard, when we consider the intent and
capabilities of our enemies, we cannot underestimate them or, as the 9/11
Commission found in a different context, suffer from failures in
imagination, policy, capabilities, or management.

Thus our future remains uncertain. Based on our increasing reliance on
networks to drive our economy and support our health, welfare,
communications, and security, certain questions loom large. For example,
can our enemies control whether, how, and when our systems operate and
our vital services get delivered? Are our personal and business records,
corporate intellectual property, and state secrets routinely exposed or
imperceptibly altered?*

Unfortunately, the answers to these questions not only remain
unknown, they perhaps are unknowable. Therefore, it is difficult to provide
our nation’s government leaders, corporate executives, shareholders, and
citizens with reasonable assurance that our computer systems have not been

* Deputy Assistant Director, Federal Bureau of Investigation.
1. Especially worrisome are the cyber attacks that would hijack systems with false
information in order to discredit the systems or do lasting physical damage. At a corporate
level, attacks of this kind have the potential to create liabilities and losses large enough to
bankrupt most companies. At a national level, such attacks directed at critical infrastructure
industries have the potential to cause thousands of deaths and hundreds of billions of dollars
worth of damage. See U.S. Cyber Consequences Unit (US-CCU), http://www.usccu.us/#
Key_Features_of_the_US-CCU’s_Research (an independent, nonprofit research institute).
penetrated, that our software has not been adulterated, and that our hardware does not contain implants. Similarly, it is difficult to state with confidence that over time our mission-critical data and systems – which underlie our economic prosperity, national security, and public health – will remain accurate and available when needed.

We do know that cyberexploitation is occurring at an unprecedented rate by a growing array of state and nonstate actors against a wide range of targets, and that the threat will continue to grow as our society becomes increasingly reliant on information systems. For these reasons, just over four months into his Presidency, Barack Obama announced that “our digital infrastructure – the networks and computers we depend on every day – will

---

2. A glimpse into the full scope of this problem is reflected in the SANS Institute’s expert consensus ranking of the top ten cyber threats:

1. Increasingly Sophisticated Web Site Attacks That Exploit Browser Vulnerabilities – Especially on “Trusted” Web Sites.
2. Increasing Sophistication and Effectiveness in Botnets.
4. Mobile Phone Threats, Especially Against iPhones and Android-Based Phones; Plus VOIP.
5. Insider Attacks.
6. Advanced Identity Theft from Persistent Bots.
8. Web Application Security Exploits.
10. Supply Chain Attacks Infecting Consumer Devices (USB Thumb Drives, GPS Systems, Photo Frames, etc.) Distributed by Trusted Organizations.


3. The full dimension of the cybersecurity problem includes not only risks to the confidentiality, integrity, and availability of sensitive data, but also substantial risks to the command and control of important physical assets such as electric power grids, water supply, and other critical infrastructure. See, e.g., DEPARTMENT OF HOMELAND SECURITY, PRIMER CONTROL SYSTEMS CYBER SECURITY FRAMEWORK AND TECHNICAL METRICS (2009), available at http://www.us-cert.gov/controlsystems/pdf/Metrics_primer_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. Consequently, control systems and the associated critical infrastructure are at greater risk than before from externally initiated cyber attacks.” Id. at 1.

4. Intelligence Community and Annual Threat Assessment: Hearing Before the Sen. Armed Serv. Comm., 111th Cong. 38 (2009) (statement of Dennis C. Blair, Dir. of Nat’l Intell.), available at http://www.dni.gov/testimonies/20090310_testimony.pdf (“As government, private sector, and personal activities continue to move to networked operations, our digital systems add ever more capabilities, as wireless systems become even more ubiquitous, and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow.”).
be treated as they should be: as a strategic national asset," to be protected as "a national security priority."

To be sure, numerous academic and professional fields have developed around cybersecurity and risk management. All is not lost. Most certainly, there is a corresponding need to guard against an overreaction to these problems that would lead to total risk avoidance at all times for all things. Yet, how many people have the data necessary to assess their vulnerabilities, the threats against them, and the harm they are facing in the event of a successful attack? Each data point is essential to establishing an accurate risk profile and, in turn, making informed decisions about how we prioritize and protect our resources. Similarly, how many directors, officers, and government leaders understand who within and outside their organization affect their risk posture? Is the systems administrator or the chief information security officer in charge? Or, as tends to be the case far too often, is the company put at risk when an employee shows up at work one morning with a thumb drive that he plugs into his desktop's USB slot?

Regrettably, we have brought these vulnerabilities upon ourselves, having first invented the Internet and then having eagerly embraced the ensuing Digital Revolution without establishing a corresponding viable security structure. This point has not been lost on FBI Director Robert Mueller, who likened our predicament to that of Ancient Rome. In 2007, Mueller said:

There is an old saying that all roads lead to Rome. In the days of the Roman Empire, roads radiated out from the capital city, spanning more than 52,000 miles. The Romans built these roads to access the vast areas they had conquered. But, in the end, these same roads led to Rome's downfall, for they allowed the invaders to march right up to the city gates.⁶

I. FRAMING A CYBERSECURITY STRATEGY

It is difficult to develop a national strategy for a subject as vast as cybersecurity. Where do we start and, perhaps equally perplexing, how do we know when to stop and move on toward implementation? From a federal government perspective, these questions were presented not long ago to the National Cyber Study Group (NCSG). The NCSG was formed by the Office of the Director of National Intelligence and began to meet

---


weekly in May of 2007. Under the skillful leadership of Melissa Hathaway, the NCSG developed in less than a year the cyber strategy that would later be adopted by the White House as the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI is contained within National Security Presidential Directive 54, which is cross-designated as Homeland Security Presidential Directive 23. That document remains classified and therefore unavailable to the public, although the White House has released an unclassified summary. Nevertheless, for purposes of this article, knowing the entirety of the policy is less important than exploring the framework used to develop, monitor, and coordinate the strategy.

II. THREAT ACTORS AND THREAT VECTORS

It has been observed wisely that while no models are perfect for developing strategy, some are at least useful. The first imperfect and ultimately useless model that NCSG members considered was to break down cybersecurity strategy into the three components of computer network operations (CNO) – namely, computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND). At first blush, this approach seemed reasonable. If policy makers

7. The NCSG consists of dozens of senior managers from across the government. The sheer number of high-level representatives seated at the table (and spilling over to the seats lined up against the walls) is a visible indicator of the magnitude of both the cyber problem set and the cyber solution set from within the federal executive branch alone. The NCSG includes members from the seventeen-agency intelligence community, the Executive Office of the President, and law enforcement, homeland security, military, and civilian departments and agencies.

8. Hathaway was later called upon by President Obama to serve as Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils, responsible for leading the 60-day interagency review of the plans, programs, and activities underway throughout the government dedicated to cybersecurity. See: "President Obama Directs the National Security and Homeland Security Advisors To Conduct Immediate Cyber Security Review (Feb. 9, 2009), available at http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/.

9. Despite the underlying breadth and wisdom of the strategy, it is a fair criticism to note that the CNCI name is overstated in its use of the term "comprehensive." Getting our nation's collective arms around the problem known generally as "cybersecurity" is difficult, if for no reason other than the dynamic nature of the global ecosystem known as "cyberspace." Policy makers cannot help but leave strategic gaps that are in need of continual review. Cybersecurity policy, like cybersecurity itself, is a process. There are no one-time solutions.


could determine which departments, agencies, infrastructure owners, and thought leaders played prominently in strategic development within these three areas, surely (the logic held) they would be well on the way to organizing new solutions.

The model broke down quickly, however. It did not take long for the NCSG to realize that the definitions of CNA, CNE, and CND are muddled, without clear legal or policy distinction, and often bleeding between themselves. One person’s CNE may be another person’s CNA, and the other way around. After all, the same root access typically used by an intruder to conduct surveillance of a network can be used by the same intruder for the purpose of shutting down the network entirely. Meanwhile, CND has been viewed by some to consist of information security officers focused on their own targeted systems and, equally, of others who would try to neutralize the threat along its route, including at its source.\(^\text{12}\) As a result, the skill sets, mission authorities, and actors underlying CNA, CNE, and CND are likely to be grouped together rather than distinguished from one another.\(^\text{13}\) Hence, for purposes of strategic development, breaking the problem down along CNO divisions turns out to be a non-starter.

Moving on, one might be tempted to consider breaking down the problem (and the response) by the identity of the threat. Such an effort would quickly lead to organizing the cyber threat into three broad categories: nation states, terrorists, and criminals (the latter two would include organized groups as well as lone offenders.). The appeal of this particular breakdown is that it aligns most closely with our nation’s executive branch authorities. Clearly defined departments or agencies are involved and have primacy, whether domestic or abroad, in the event of a state-sponsored act of war or espionage against our government or private sector interests, and similar distinctions emerge under both law and executive orders in the event of terrorist or criminal activity.\(^\text{14}\) The trouble

---

\(^{12}\) Id. “Computer Network Defense” (CND) is “[a]ctions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.” Id. “Computer Network Exploitation” (CNE) is defined as “[e]nabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.” Id.

\(^{13}\) By way of example, military doctrine describes the term “active defense” as “[t]he employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.” Id. at 4.

\(^{14}\) See, e.g., Adam Stump, Vice Chairman Cites Need for Cyber Warfare Experimentation, DEFENSE LINK, June 20, 2008, available at http://www.defenselink.mil/news/newsarticle.aspx?id=50273 (reporting on remarks made by Vice Chairman of the Joint Chiefs of Staff, Marine Corps Gen. James E. Cartwright, about building a military force that has both the ‘defend and operate skills’ and the ‘exploit and attack skills.’).

---

with spending time approaching policy from the perspective of the adversary’s identity, however, is that it is either meaningless or difficult to implement in practice. Our networks are almost indistinguishably vulnerable to a wide array of nation states, terrorists, and criminals (all of whom may interact with one another). Thus our network defenders are not substantially assisted by emphasizing jurisdictional or policy factors. Moreover, attributing a specific cyber event to a particular actor remains difficult by design.  

Ultimately, the NCSG settled on a rather elegant solution to the cybersecurity problem. Rather than first focus on CNO or threat actors, the group charted out the cyber threat vectors. It turns out that the threat vectors fall rather neatly into four broad categories: supply chain and vendor access, remote access, proximity access, and insider access.

With respect to the supply chain, it is widely accepted that the global economy has given our nation the ability to compete and purchase services in an expanded market that has driven down prices and promoted rapid invention and innovation. Unfortunately, the global supply chain also has substantially increased our vulnerability to adversarial manipulation of our software and hardware. Straight out of the box, our computers (or the architecture they ride on) can be poisoned with dormant capabilities that can be awakened by those who do not have our best interests at heart. Equally true, our technology systems can come out of the factory in pristine condition, only to be manipulated by the delivery service, the wholesaler, the retailer, the installer, the repairman, or through the downloadable firmware update or patch. Supply chain and vendor operations are very difficult to monitor and can compromise us entirely. Moreover, even without a global supply chain, these same exploits could be introduced domestically by organized crime groups, disgruntled employees, or foreign intelligence officers operating inside of our country. Hence, inevitable calls for protectionism must be considered within this larger, more difficult context. Fortunately, numerous ongoing efforts, including the CENC’s Initiative 11, have identified and are seeking to address these and related concerns.

(Defining law enforcement jurisdiction and federal criminal offenses).

15. For a variety of significant reasons, we have embraced interoperable standards and technologies that permit anonymity while shunning technologies that promote identification. Thus, arguably, we have made the process difficult, even though in theory one could not imagine a process that lends itself more readily to perfect attribution than does a point-to-point communication medium such as the Internet. After all, every communication that travels through cyberspace has a definite start point and end point.

The next avenue of attack to consider is remote access or, in common parlance, computer network intrusions or “hacking.” We see the most of this threat vector either because it is the greatest problem or because it is the most easily tracked. Systems Administrators typically are overwhelmed by the quantity of warnings issued by automated intrusion detection, prevention, and firewall systems, and by the additional need to study the logs associated with other technology services and applications. Indeed, the National Institute of Standards and Technology (NIST) correctly observes that our visibility into remote access security incidents is so great that an organization must prioritize its review and response efforts. Hacking, together with the associated methods for obtaining remote access provided by malicious email attachments and drive-by downloads might or might not be the worst of our problems, but they certainly are the most visible. From a strategic point of view, it is important to ensure that the volume of the perceived remote threat and the resources directed against it are not considered to the exclusion of other equally pernicious threat vectors. Even if we were able to prevent all remote intrusions and remote attacks, we still would have trouble – a lot of it.

17. As used in this article, the term “hacking” refers to the act of unlawfully accessing a computer entirely without authorization, or accessing data or functions on a computer in a manner that exceeds authorization. As a matter of U.S. federal law, the principal statute that criminalizes hacking and related cyber offenses is 18 U.S.C. § 1030. For purposes of strategy, Distributed Denial of Service (DDoS) attacks are best considered within the “remote access” category, even though they do not necessarily involve “access” into a computer system.

18. As observed by the NIST, from a market standpoint, complete log analysis by any individual company may lack a sufficient return on investment to justify the effort:

   One of the challenges to the effective management of computer security logs is balancing the availability of large amounts of log information with the limited availability of organizational resources for analysis of the data. . . . Organizations could realize benefits in using the data to reduce risks, but the staff time and resources needed to perform the analyses and to manage the log information have to be taken into consideration.

“Proximity access” refers to the abilities our adversaries have when they are physically close to our networks but not directly inside them. The interception of wireless signals is a good example of this vector. Through common techniques such as wireless sniffing (passive electronic monitoring of information being transmitted through wireless), peer-to-peer connections (joining a wireless connection and obtaining the ability to access other computers connected to the same wireless network), and “evil-twin attacks” (the attacker poses as a legitimate wireless network in order to lure unsuspecting users), wireless connected devices and wireless access points can turn into a significant cybersecurity liability. Wireless keyboards can present similar opportunities for eavesdroppers, broadcasting keystrokes through the air, even user IDs and passwords. Of course, high-tech gadgets are not needed to engage in close access operations. The term “shoulder surfing” has been used to describe the risk to private data posed by the bad guy who simply casts his eyes on an unsuspecting user’s keyboard or monitor.

Finally, insider access must be addressed. Current employees, contractors, and trusted business partners have a unique opportunity to do us harm because they have been provided authorized access to our physical and digital spaces. Once authorized, they can operate from within the “soft gooey center” without being challenged by the “hard outer shell” of gates and guards, intrusion prevention systems, and firewalls. Operating from the inside also provides a distinct perspective on a company’s security weaknesses, including technical gaps, lapses in policy enforcement, knowledge of where the crown jewels are located, and even vacation schedules of security staff, just to name a few. Although a cyber attack is more likely to come from an outsider, research indicates that when an insider does strike, the damage may be substantially greater.

The insider threat is usually recognized as including intentional employee fraud, theft of intellectual property, and information technology sabotage, whether at the hands of disgruntled employees, those seeking illicit financial gain, or those seeking business or nation state advantage. In addition though, it makes practical sense to consider the insider threat as also embracing well intentioned employees whose conduct unintentionally causes or contributes to a breach. After all, whether through socially engineered emails or the exploitation of default passwords, our adversaries

20. Id.
22. See, e.g., DAVID CAPPELLI ET AL., COMMON SENSE GUIDE TO PREVENTION AND DETECTION OF INSIDER THREATS 5-6 (3d ed. 2009).
routinely take advantage of the predictable security failings of employees, and in this way defeat our expensive perimeter defenses.

III. STRATEGIC CHALLENGE: CONSIDERATION OF RISK FACTORS

Recognizing the full extent of these threat vectors is a necessary first step, but it represents only one part of the strategic equation. In order to lower the security concerns that each of these vectors poses, it is helpful to introduce the concept of risk. The classic risk formula is a useful guide in this regard: Risk = Threat x Vulnerability x Consequence.

Two basic theoretical truths emerge from this formula that are useful from a strategic perspective, regardless of whether the equation itself is susceptible to practical application or whether actual values can be provided with ease for each of the variables in a particular setting. First, lowering any of the three variable factors (threat, vulnerability, or consequence) will lower the risk. Second, driving any of the three factors to zero will eliminate the risk altogether because, through multiplication, “R” will become zero if any variable is zero (this is the rationale for using multiplication in the equation rather than addition.).

These points taken together lead to the following conclusions: if any one variable can be brought to zero, all things being equal, that is the most effective security path to take; once a variable is brought to and permanently maintained at zero, it is not cost effective to pursue either of the other factors; and, if none of the variables can be brought to zero, a defense-in-depth approach — focused on lowering each of the three factors — should strongly be considered. To be sure, there is always a point where the costs of seeking to eliminate or even reduce a particular risk (or variable) will outweigh the benefits, thus leading to valid and necessary risk management considerations.

A couple of examples outside the cyber context help drive home the point. First, consider the risk we all face each summer from garden variety mosquitoes. Cycling through each of the three factors, we could go after the threat by putting up a bug zapper to kill or repel each mosquito. Alternatively, we might allow at least some mosquitoes to live and instead focus on reducing the mosquito victim’s vulnerability to being bitten.

23. The underlying assumption, which must be validated as applied to a particular scenario, is that lowering a particular variable does not have the unintended consequence of raising either of the other two variables.

24. See, e.g., ROD BECKSTROM, NATIONAL CYBERSECURITY CENTER, DEPARTMENT OF HOMELAND SECURITY, A NEW MODEL FOR NETWORK VALUATION 1, 6-7 (2009), available at http://www.beckstrom.com/images/networks.pdf (applying Beckstrom’s Law to demonstrate that “the net benefit value of a network is equal to the summation of all transaction benefits, less all transaction costs, less security costs, and less security related losses to a user,” and observing: “One dollar of security investments is only a benefit when it reduces expected losses by more than a dollar.”).
Wearing DEET or long-sleeve shirts and pants or sitting within a net-covered area all come to mind as valid approaches. Finally, if some mosquitoes will live, and self-defense is uncomfortable or impossible, managing the consequence of mosquito bites might be achieved through the application of calamine lotion. Still, a good number of people will fail to ward off the mosquitoes, decide not to wear appropriate clothing or chemicals, and not be prepared with calamine lotion. They will have treated the costs of mosquito defense as outweighing the benefits. They take their chances, itch, scratch, and recover. Would their calculus change if mosquitoes carrying dengue fever came to town? You bet it would.

Next, consider the risk involved in hiring a house-cleaning service. Perhaps you saw an advertisement and find the service affordable. Yet, there remains a nagging sense that allowing a stranger full access to your home could result in theft or damage. Using risk analysis, you would break down the problem into its three component parts and focus on ways to drive down the threat, reduce the vulnerability, and because the first two might fail, eliminate negative consequences. Reducing the threat likely could include performing a background check on the applicant, obtaining references, and seeking referrals. Surely the overall risk of theft or damage may be lowered by reducing the likelihood that the threat actor (the potential housekeeper) will steal or act carelessly. Alternatively, or in addition, the overall risk would be lowered by reducing the likelihood that vulnerable targets (household possessions) are subject to being taken or damaged. Storing as many valuables as possible in a safe might help achieve this result, as would removing them from the house. Finally, unless the homeowner can have complete confidence in the housekeeper's character and capabilities (thus reducing the threat), or is able either to remove everything fragile and of value or lock them in a safe (mitigating the vulnerability), the overall risk of theft or damage may be lowered by mitigating the consequence of theft or damage. For replaceable items, obtaining homeowners insurance would fit the bill, as would hiring a cleaning service that is insured and bonded. Of course, in any given situation, the value of the goods that might be broken or stolen may not justify the additional costs of hiring only known individuals from reliable cleaning services, purchasing a house safe, and obtaining homeowners insurance. If that is the case, it might make sense to accept the risk.

IV. DIAGNOSING CYBERSECURITY VECTORS AND RISK

Turning to cybersecurity, our shared challenge is to apply risk analysis to each of the four threat vectors previously discussed. Thus, anybody involved in cybersecurity strategy, law, policy, or research would do well to take the "Cybersecurity Vectors and Risk" chart printed below and attempt to complete it. Typically, each of the twelve cells requires active engagement.
Reducing the cybersecurity threat means focusing either on preventing or deterring the adversary from acting. Preventing the adversary from acting might include law enforcement, diplomatic, intelligence, or military efforts to neutralize the individuals (kill, capture, or cajole), or their tools (deny, destroy, or disassemble). Deterring the adversary from acting could include an even wider array of options, depending on the particular adversary. Rational adversaries presumably engage in their own cost/benefit analysis, which would be affected by sticks (for example, threatened law enforcement, military, diplomatic, social, or economic sanctions), carrots (perhaps economic opportunities or enhanced social standing for lawful use of offensive skills), or futility (if the threat actor successfully exploits a vulnerability but does not obtain the expected benefit).

Addressing cybersecurity vulnerabilities requires a focus on hardening the targets, whether through supply chain management, better design, information security practices, education, or other means. Absolute protection is not required. Surely, for example, it would be a great benefit if we could reduce our vulnerabilities to the point that only the most sophisticated nation states could exploit them. Not only would that reduce the number of incidents, it would also limit the field for determining attribution should we observe a security event (which itself would serve as a deterrent to those nation states whose current activities rely on anonymity and blending in with the noise of criminal activity).

25. From a risk management perspective, it is important to remain mindful that even when a pre-positioned adversary does not have the intent to act, systems or data may be inadvertently compromised through negligence or recklessness. For example, whether or not those distributing the vast array of malicious software currently residing throughout our networks intend to inflict harm, it is obvious that their creations have not been beta-tested to avoid unintentional disruption.

26. Beckstrom, supra note 24, at 2, 9 (referring to hacker economics).
Finally, consequence management requires a focus on minimizing the harm that results when an adversary takes advantage of an existing weakness. Cyber events must be included within Incident Response and Continuity of Operations plans in order to limit losses to life, property, privacy, public health, business operations, and confidence. Efforts in this space might seek to limit the actual loss in the first instance (for example, by encrypting data or removing the most sensitive data to more secure systems), or might seek instead to "play through" the loss by having the ability to restore the situation to an acceptable state, perhaps by maintaining redundant equipment (such as alternative communications channels), data (including offsite back-ups), processes (including command and control systems), and personnel (via succession planning and the geographic distribution of leadership). 27

Notably, there are almost always opportunities to share contributions or knowledge from one risk factor discipline for the benefit of work being done by others. For example, those who pursue our adversaries are typically exposed to their motives, intentions, tactics, and techniques, each of which is relevant to those focused on reducing vulnerabilities to exploitation or attack, or on limiting the consequences of a successful intrusion or attack. After all, an adversary’s target list not only assists in prioritizing defensive efforts, but may also identify vulnerabilities of which the target was unaware, or suggest that certain consequence management efforts would be ineffective. Similarly, those who are most likely to be victimized by cyber attacks have relevant information for those seeking to reduce the threat, as well as for those planning for recovery and continuity, and vice versa.

Not all information can be shared for all purposes. There are legitimate legal, policy, and business reasons that prevent those who would enhance our nation’s security from sharing all they know with one another. Still, for the reasons discussed here, identifying those impediments and seeking to resolve them must remain a priority.

CONCLUSION

Current trends towards digitization, automation, and interoperability need not be mutually exclusive of security. However, the cybersecurity challenge can only be addressed effectively by fully understanding the wide range of threat vectors. Even then, these concerns can only be efficiently resolved by seeking the best options for lowering each of the three risk factors. Policymakers, strategists, and those who operate on the front lines


-344A152BE286EA358525714200618BCD
of cybersecurity should carry out their direct and indirect roles in ways that help to lower the threat, vulnerability, and adverse consequences associated with supply chain and vendor access, remote access, proximity access, and insider access. Anything less leaves the advantage with our adversaries.
petitioners were convicted in the District Court for the Western District of Washington of a conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting and importing intoxicating liquors and maintaining nuisances, and by selling intoxicating liquors.

Olmstead was the leading conspirator and the general manager of the business. There were telephones in an office of the manager, in his own home, at the homes of his associates, and at other places in the city. The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators.

The argument of the defense was that the wiretap was illegal. The statute of Washington, adopted in 1909, stated that:

"Every person . . . who shall intercept, read or in any manner interrupt or delay the sending of a message over any telegraph or telephone line . . . shall be guilty of a misdemeanor."

The holding of the Court was instructive for the era:

"The common law rule is that the admissibility of evidence is not affected by the illegality of the means by which it was obtained. We think, therefore, that the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment."

The majority went on to say that:

"The evidence was secured by the use of the sense of hearing, and that only. There was no entry of the houses or offices of the defendants."

The 4th Amendment was clearly thought to be a property-based rule of law. Mr. Olmstead went to jail.

Today, the most important part of the Olmstead case was not the majority finding, but that of the dissent by Justice Brandeis. Justice Brandeis wrote:

"The Government makes no attempt to defend the methods employed by its officers. Indeed, it concedes that, if wiretapping can be deemed a search and seizure within the Fourth Amendment, such wiretapping as was practiced in the case at bar was an unreasonable search and seizure, and that the evidence thus obtained was inadmissible. But it relies on the language of the Amendment, and it claims that the protection given thereby cannot properly be held to include a telephone conversation."

Brandeis basically believed that the 4th Amendment really meant that the "people" had a right to be left alone:

Privacy, Technology, Security, and Surveillance

by M.E. (Spike) Bowman

"Furnished as all Europe now is with Academies of Science, with nice instruments and the spirit of experiment, the progress of human knowledge will be rapid and discoveries made of which we have at present no conception. I begin to be almost sorry I was born so soon, since I cannot have the happiness of knowing what will be known a hundred years hence."

— Benjamin Franklin

The Legal Background

This article is loosely about the 4th Amendment and what it might mean in an era of technology never contemplated by the Framers. More to the point, it is about the way technology has changed and is changing the way we live our lives and, perhaps, the way the 4th Amendment is understood. The issues have to do with what we want the government to do to protect us — or, on the flip side of that question, to what extent are we comfortable with the government (and private industry) peeking into our private lives. It is no surprise that the law has much to do with how society orders itself, but today technology is pushing the limits of our expectations of the law. Today, privacy collides with security in unexpected ways and we find that the law struggles to keep up with evolving social issues.

It is useful to look at what the 4th Amendment has meant through the years. Importantly, the 4th Amendment went with little or no controversy for more than a century in the United States. The seminal case ushering in the modern era of interpretation came in 1928. United States v. Olmstead1 was a case in which...
"When the Fourth and Fifth Amendments were adopted, "the form that evil had theretofore taken" had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly effect (sic) self-incrimination."

More importantly, Justice Brandeis anticipated the future:

"The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions."

The next relevant action for purposes of this article occurred in 1934. The Federal Communications Act recognized that telephone communications had become so commonplace, and so important to ordinary communication that society had come to expect that they should be private. Accordingly the Act provided that interception without competent authority would be unlawful. The concept of privacy was not ripe for the time, but the importance of the telephone had come of age.

It is appropriate, at this point, to skip forward a number of years to look at the 1942 criminal case, Goldman v. United States, Shulman v. SAME. The petitioners and another were indicted for conspiracy to violate § 29(b)(5) of the Bankruptcy Act. Petitioners were tried and convicted based in large measure on conversations intercepted by technical means.

Two federal agents had a detectaphone having a receiver so delicate as, when placed against the partition wall, to pick up sound waves originating in Shulman's office, and means for amplifying and hearing them. With this, the agents overheard, and the stenographer transcribed, portions of conversations and also what one of the conferees said when talking over the telephone from his office.

Petitioners appealed the conviction based on a claim of a violation of the 4th Amendment but also on a claim that the Federal Communications Act of 1934 had been violated. Their argument was that a communication falls within the protection of the statute once a speaker has uttered words with the intent that they constitute a transmission of a telephone conversation. The Court held that (1) the overhearding and divulgence of what was spoken into a telephone receiver was not a violation of § 605, that (2) what was heard by the use of the detectaphone was not made illegal by trespass or unlawful entry, and (3) that the use by federal agents of a detectaphone, whereby conversations in the office of a defendant were overheard through contact on the wall of an adjoining room, did not violate the Fourth Amendment (relying on Olmstead).

The next relevant event was a 1961 criminal case, Silverman v. United States. Silverman was a case not terribly dissimilar to Goldman. In this case petitioners were convicted of gambling offenses under the District of Columbia Code. Admitted in evidence over their objection was testimony of police officers describing incriminating conversations engaged in by petitioners at their alleged gambling establishment, which the officers had overheard by means of an electronic listening device pushed through the party wall of an adjoining house until it touched heating ducts in the house occupied by petitioners. What was different from Goldman is the fact that eavesdropping was accomplished by means of an unauthorized physical penetration into the premises occupied by petitioners, which violated their rights under the Fourth Amendment (citing Goldman). In the Goldman case there had been no penetration of the petitioners' property; in Silverman there was - reaffirming the property-based analysis of the 4th Amendment.

Then, in 1965 the beginning of a sea change in policy and law occurred with a case that had nothing in common with the Olmstead lineage. Griswold v. Connecticut was a case in which appellants, the Executive Director of the Planned Parenthood League of Connecticut, and its medical director, a licensed physician, were convicted as accessories for giving married persons information and medical advice on how to prevent conception and, following examination, prescribing a contraceptive device or material for the wife's use. A Connecticut statute made it a crime for any person to use any drug or article to prevent conception. Appellants claimed that the accessory statute, as applied, violated the Fourteenth Amendment. An intermediate appellate court and the State's highest court affirmed the judgment. Somewhat unusually, the Supreme Court agreed to take a case that dealt solely with one state's law. There were several issues involved in deciding the case, but only one is relevant to this discussion - in Griswold the Court found a Constitutional right to privacy.

"The present case, then, concerns a relationship lying within the zone of privacy created by several fun-

---

4. 381 U.S. 479 (1965).
damental constitutional guarantees.... We deal with a right of privacy older than the Bill of Rights — older than our political parties, older than our school system. Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred. It is an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects. Yet it is an association for as noble a purpose as any involved in our prior decisions."

In a divided Court the majority opinion referred to several other instances in which there had been found a right to privacy and solidified the concept, essentially laying down a new precept when it held that privacy was in the penumbra of the Constitution, citing, as examples the 1st Amendment right to be free of government intrusion and the 4th Amendment’s guarantee against unreasonable searches and seizures. As noted, this was not the first time the Court had found a right of privacy but it was the most conclusive finding that privacy was a precept that lay within the confines of the Constitution. This was to have a far-reaching effect in very short order.

Two years later, in 1967, a Mr. Katz was convicted under an indictment charging him with transmitting wagering information by telephone across state lines. Evidence of petitioner’s end of the conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the telephone booth from which the calls were made, was introduced at the trial. The Court of Appeals affirmed the conviction, finding that there was no Fourth Amendment violation, since there was "no physical entrance into the area occupied by" petitioner. Katz is a hugely important case for several reasons but here we concentrate on one issue only — privacy.

The Court’s majority opinion reflected on the years of 4th Amendment rulings stemming from the Olmstead and Goldman cases, as well as the differently decided Silverman case. It further reflected on the fact that the Court had found rights of privacy, determined by individual facts, in a number of cases since the Olmstead decision. In a sweeping break from precedent the Court concluded:

We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth, and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.

The essence of the case was that Katz had entered a telephone booth, closing the door with a reasonable expectation of privacy. Despite the fact that the agents were relying on Olmstead and acted with reasonable restraint, the Court held that the essence of the 4th Amendment requires that they should have obtained authorization from an impartial magistrate. In a concurring opinion Justice Harlan expressed the fundamental issue in a way that has come to be accepted doctrine:

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."

5. The magnitude of the break is illustrated by a short paragraph from the dissent of Justice Black: "My basic objection is twofold: (1) I do not believe that the words of the Amendment will bear the meaning given them by today’s decision, and (2) I do not believe that it is the proper role of this Court to rewrite the Amendment in order to bring it into harmony with the times," and thus reach a result that many people believe to be desirable." 389 U.S. 362.

Advances in Technology

The reason that the legal background is necessary begins to show itself in a program called SHAMROCK.7 Shamrock started innocently enough. It was a program dating back to the 1940s by which the National Security Agency desired to (1) maintain cryptologic skills and (2) understand who might be communicating with persons abroad with whom we might have concerns. Succinctly, the FBI would go to the major cable companies and collect copies of cables of interest. The cables were created with 4-ply paper. One sheet was used to send the cable, one was the record copy, one was the customer copy and the 4th copy went in the trash. Under the law, that was abandoned property so there was no concern with the program.

As time passed, technology improved and eventually computers took over the mechanical processes of sending cables. Magnetic tapes were used instead of paper but the NSA practice continued as the FBI would simply ask for copies of the magnetic tape. The program proved to be so successful with the magnetic tapes that there seemed to be limitless possibilities for its use — the analytical possibilities were improved by orders of magnitude over the old paper copies. Eventually, under then Attorney General Bobby Kennedy, the program was turned to domestic uses and even used to gather information about notables like Martin Luther King.

The process had evolved so naturally that little thought was given to the fact that the magnetic tapes were not “trash,” and therefore were not free for the taking. The analytical possibilities were so great that it seemed natural to use the program for domestic rather than just national security reasons. Without conscious thought a program that had been a highly restricted foreign policy and perfectly legal initiative had transitioned to a behemoth of quite a different character, occupying quite a different legal dimension.

SHAMROCK was exposed at a time when national suspicion of the intelligence community was at an all-time high. In 1975, Senator Frank Church of Idaho headed an investigative committee focused on the intelligence community.8 When it had finished it had compiled several volumes of information running to many thousands of pages. They found waste, duplication of effort, unlawful activities, experimentation on humans, assassination plots and many other suspect issues, but read thoroughly the greatest volume of findings had to do with the violations of privacy. The Privacy Act9 was only two years old but already privacy had occupied a niche in the American social conscience.

At this point yet another Supreme Court case enters into the technology/privacy scene. Smith v. Maryland10 was a case in which the telephone company, at police request, installed at its central offices a pen register11 to record the numbers dialed from the telephone at petitioner’s home. Prior to his robbery trial, petitioner moved to suppress “all fruits derived from” the pen register. The Maryland trial court denied this motion, holding that the warrantless installation of the pen register did not violate the Fourth Amendment. Petitioner was convicted, and the Maryland Court of Appeals affirmed.

Smith appealed on 4th Amendment grounds but the Court, relying on the Katz case found no legitimate expectation of privacy.

“First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of law." . . . Second, even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as reasonable."

The holding of the Smith case is critical for more than Mr. Smith’s liberty. What Smith v. Maryland stands for is that if you give your information to a third party you have given up any reasonable expectation of privacy. At this point it is reasonable to ask whether this holding permits the searches of e-mail subject lines and URLs. How about the use of new technologies such as GPS tracking devices, radio frequency identification chips in passports and consumer goods,

8. United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities.
9. 5 USC 552 (a).
11. A pen register records the calling data (not voice) of outgoing phone calls. A trap and trace records the data of incoming calls.
biometric surveillance, or whole-body backscatter x-ray in public places?

Today information that was not previously available to third parties is a key stroke away from exposure — privacy has become a casualty of technology. However, one has to ask just what privacy means today because it is such a nebulous concept that it means many things to many people. When we give up so much personal data on Facebook it becomes clear that the concept is attenuated with many. Technology, in only a few short years, has changed social patterns without our really realizing what has happened.

Consider for a moment facial recognition technology. Only a few short years ago this technology was in the realm of science fiction. Today a camera phone application that finds names and addresses of total strangers is a stalkers dream. The facial recognition “app” instantly identifies snaps by matching them to photos on websites like Facebook and Twitter where personal information can be accessed. Burglars taking secret snaps of revelers could find addresses. Unsuspecting strangers fooling around on nights out could fall prey to blackmail. A guy could take a picture of a girl in a bar and discover all manner of information about her.

The smart phone does more than take pictures. Consider the information we all store on these devices and it is easy to realize that it is just too user friendly. It has our call logs, photos, videos, and text messages. It has our Web history, typically holds passwords for Web services and accounts. It retains records of cell towers it contacts so it has your location history, often for months past. iPhone’s Siri is storing one of our biometrics – our voices. Strong passwords are a must to protect this data, but even then it is not safe from law enforcement which has been known to send locked phones to Apple and Google which extract the information and return it on a DVD.

What do retailers know about you? We have become accustomed to retail services tracking our interests for marketing purposes, but it is an invasion of privacy that wasn’t possible only two decades ago. Today retailers are beginning to use cameras for the same purpose and to identify criminals. Retailers are introducing mannequins designed to observe customers and discern their interests and to feed data into facial recognition software and to log age, gender and race. Or consider what data aggregators such as ChoicePoint know about you.

ChoicePoint is a Georgia-based company that combines personal data sourced from multiple public and private databases for sale to the government and the private sector. The firm maintains more than 17 billion records of individuals and businesses, which it sells to an estimated 100,000 clients, including 7,000 federal, state and local law enforcement agencies (30 March 2005 estimates). While ChoicePoint sells data responsibly, it has suffered several security breaches which have led to the theft of the personal information it holds. The truly vast amount of information it gathers on individuals is not collected pursuant to any guidelines, and it can be sold as any merchandise could be sold.

Next, consider the amount of information we disclose on social media and what can be done with it. The Federal Reserve Bank has issued a “Request for Proposals” seeking a contractor to sample social media to determine the nation’s economic mood. The FBI is sponsoring a wide dispersal of facial recognition software to aid local police in identifying unknown individuals. The Department of Defense is seeking software to sample social media in order to track how groups interact and evolve.

Just what is available on social media? Facebook has 900 million profiles — if it were a country it would be the third largest in the world. At least 100 million images and 60 million updates are added to Facebook each day. Facebook and other social networks collect enormous amounts of highly sensitive information and distribute it more quickly and widely than traditional consumer data-gathering firms ever could. Moreover, posting private information on a public site relinquishes privacy interests.

In 2011 Ivan Kaspersky, son of the famous Russian data management and security expert was kidnapped. His father blamed it on “VK” — the Russian form of Facebook. Kaspersky said that the Russian social network had tempted Ivan into posting his address, phone number and even details of an internship at a security company.
“WeKnowYourHouse” is an application that scours Twitter for people using the word “home in their tweets and picks up their associated geolocation then publishes the tweet to its own site along with information about where the tweeter is. With that information the site uses Google Streetview to post an image of what may be the person’s home.

Looking to the future, technology may well outstrip even the wildest imagining of Justice Brandeis. Even now, the Defense Advanced Research Projects Agency (DARPA) is teaming with Carnegie Mellon University to create an artificial intelligence system that can watch people and predict where a person will “likely” do in the future. The vision is that the system will use special programmed software designed to analyze various real-time video surveillance feeds to automatically identify and notify officials when an action not permitted is detected.

Transit authorities in cities across the country are quietly installing microphone-enabled surveillance systems on public buses that would give them the ability to record and store private conversations, according to documents obtained by a news outlet. The systems are being installed in San Francisco, Baltimore, and other cities with funding from the Department of Homeland Security in some cases.

Increasingly, security cameras are a part of our existence — London has become famous for them. Whatever the benefit of security cameras, they create a new vulnerability. Over a year after it emerged, businesses and consumers were exposing themselves to being snooped upon when researchers uncovered a flaw in some IP security camera that let Internet users access feeds. It appears the lessons have not been learned.

Security researcher Adrian Hayter told V3 that he was able to access hundreds of publicly accessible IP camera feeds via a simple spot of Googling and a bit of knowledge about what to look for. He used the results to create a snapshot of the feeds available — which included cameras targeted at mundane subjects, like parking lots, to ones focused on strip club stages and even on babies’ cots. Hayter manually checked the feeds he discovered to remove any ones pointing at children’s beds or cots — but others may not be so scrupulous.

“The feeds inside people’s houses obviously create privacy issues,” he said. “Work-based cameras could be used in social engineering attacks.”

In a similar type of intrusion, a man recently was at a Target store purchasing nicotine patches for his son who was trying to quit smoking. At checkout he was asked for his driver’s license to verify age (he was 57) and was told by the checkout lady that she needed to scan the document. When he declined a manager first told him it was required by law and then changed the story to it being store policy.

The reason is simple. Target, and other stores want to learn all it can about you. For decades, Target has collected vast amounts of data on every person who regularly walks into one of its stores. Whenever possible, Target assigns each shopper a unique code — known internally as the Guest ID number — that keeps tabs on everything they buy. Stores record use of a credit card or coupons, the surveys you fill out and your web site visits to try to learn all they can about you.

What Does It All Mean?

Big Brother in the form of an increasingly powerful government and an increasingly powerful private sector will pile the records high with reasons why privacy should give way to national security, to law and order, to efficiency of operation, to scientific advancement and the like.

— Justice William O. Douglas,
Former Supreme Court Justice

For one thing it means that we really don’t enjoy the privacy we thought was ours when the Privacy Act was passed in 1974. Privacy is rarely lost in one fell swoop. It erodes over time, with little bits dissolving almost imperceptibly until we finally begin to notice how much is gone. Privacy is often threatened not by a single egregious act but by the slow accretion of a series of relatively minor acts. Technology has been an accelerator of this process and for the most part it has been technology that we like, technology that has made our lives easier so we have paid scant attention to the unintended consequences of these advances.

For example, today, we live much of our lives online. We make friends, receive news, execute purchases, conduct business, create documents, store photographs and find entertainment on the Internet. All of these interactions create records in the hands of third parties about our interests, problems, loves and losses, finances, associates, family moments, and even our location at any moment.

In days past, law enforcement could obtain this information only with an enormous expenditure of resources. It had to tail suspects and query informants. Consequently, the public could have some confidence that when law enforcement officers sought such personal information, they would have strong evidence
of a crime and focus their evidence collection on people likely tied to that crime. Today, the advance of technology has made it cheap and easy to gather this information secretly. The friction in the system and the practical anonymity that protected privacy are dissipating, all made possible by the third-party records doctrine of Smith v. Maryland.

In 2010 a three-judge panel of the District of Columbia Circuit Court created a split in federal circuits when it ruled that police cannot use a Global Positioning System device to track a person's movements for an extended time without a warrant, clearing the way for the Supreme Court to decide the privacy impact of the new surveillance technology in products such as cellphones and vehicle-navigation systems.12

U.S. Circuit Judge Douglas H. Ginsburg, writing for a unanimous and ideologically diverse panel, said such surveillance technology represents a leap forward in potential government intrusion that violates constitutional protections against unreasonable searches.

“A single trip to a gynecologist’s office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.”... “A person who knows all of another's travels can deduce whether he is a weekly churchgoer, 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.”

This case paved the way for a landmark decision in the Supreme Court.13 Law enforcement for years had used “slap-on” GPS devices to track the movement of suspects on the theory that there was no “intrusion” into the car and the movements of the car were plainly visible for all to see. On Certiorari, the Supreme Court unanimously ruled that the police violated the Constitution when they placed a Global Positioning System tracking device on a suspect’s car and tracked its movements for 28 days.

While the majority held that the installation of a GPS device followed by its tracking was a Fourth Amendment search, it declined to say whether that search was unreasonable and required a warrant and returned the case to the District Court to determine whether there existed a reasonable expectation of privacy.

On remand the government is arguing that the information obtained was third party data. Probably anticipating that argument, Justice Sotomayor, in a concurring opinion, said that “it may be necessary for the court to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”

In a related case, the Obama administration argues that law enforcement must regain the ability to use GPS tracking devices without a warrant, which it says is necessary to continue the fight against terrorism. Of course the January 2012 opinion in Jones appears to have held the use of GPS devices in warrantless snooping illegal. However, the administration’s brief in U.S. v. Katsin goes even further than just arguing for law enforcement’s access to the technology: the administration says vehicle-tracking is necessary to keep the nation safe from terrorist attacks, as well.

It is clear that third party data is going to be a continuing issue. After all, at the time that Smith v. Maryland was adopted there was no email, and people communicated primarily by land-line, corded telephones, fax and letter. There was no World Wide Web—if you wanted to find merchandise, you used the Yellow Pages. Cellular telephones were the stuff of science fiction. To put the period in perspective, the Vietnam War was winding down, Americans heard their music on eight-track tapes, and the Chevy Nova and Ford Maverick were the leading car models.

Recently, the Sixth Circuit took on this issue in recognition of the changed ways that we live our lives today.14

Steven Warshak owned and operated Berkeley

---

Premium Nutraceuticals, Inc. (Berkeley) which sold, among other products, an herbal supplement marketed as a pill for natural male enhancement, called Enzyte.

In 2001, Berkeley launched Enzyte and by 2004, Berkeley’s annual sales approached $250 million, in large part due to the success of Enzyte. Enzyte was marketed extensively, and approximately 98% of the advertising was done on television featuring a character known as “Smilin’ Bob.” In the script, customers signing-up for a free trial were informed that they were being enrolled in an “auto-ship” program which would charge their credit card at the end of the first prescription period and send them a refill for their current prescription. To end this auto-shipping, customers had to opt-out of the program. This program led to a large number of consumer complaints filed against Berkeley.

The auto-ship program and customers’ dislike for this practice resulted in many orders being canceled. The canceled orders hurt Berkeley’s reputation among banks and credit card companies who became reluctant to extend credit to Berkeley. To combat this, Warshak invented various ways of reducing the apparent percentage of refunded charges through questionable tactics. One tactic was to charge the customer’s account multiple times for the same purchase, once for the purchase of the supplement and another time for shipping. Warshak referred to this as “double ding.” Later, he instituted the practice of “triple ding” as well. Additionally, to secure other lines of credit, Warshak provided false information to banks.

Much of the information about Warshak’s questionable activities was contained in his email correspondence. In conjunction with a criminal investigation of Warshak and his questionable business practices, the government seized roughly 27,000 private emails from Warshak’s ISP.

Warshak was convicted and he appealed on 4th Amendment grounds. The United States Court of Appeals for the Sixth Circuit held that government agents violated the defendant’s Fourth Amendment rights by compelling his Internet Service Provider (ISP) to turn over his emails without first obtaining a search warrant based on probable cause. However, constitutional violation notwithstanding, the evidence obtained with these emails was admissible at trial because the government agents relied in good faith on the Stored Communications Act (SCA). The court then went further to declare that the SCA is unconstitutional to the extent that it allows the government to obtain emails without a warrant.

This case is notable because it is the first court from a United States Circuit Court of Appeals to explicitly hold that there is a reasonable expectation of privacy in the content of e-mails stored on third party servers and that the content of these emails is subject to Fourth Amendment protection.

In its analysis, the Sixth Circuit found that Warshak had a reasonable expectation of privacy in his e-mails and that e-mail communication had become so commonplace that privacy of e-mails is a reasonable expectation of privacy by society in general. In essence, the Court found no reasonable distinction between a letter and a communication, despite the fact that the content of e-mails is located on third-party servers.

Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.

This represents only one Circuit Court but it is, at once, a reflection of the thought process behind the 1934 Federal Communications Act and a clear challenge to the traditional understanding of the significance of third-party data (and one that Justice Sotomayor will surely welcome). A similar holding was recently issued from the Ninth Circuit Court of Appeals.

United States v. Cotterman is a case stemming from a border search of electronics. Mr. Cotterman had driven from Mexico into an Arizona port of entry site where he was questioned by border agents who seized a laptop. There had admittedly been nothing particu-
larly suspicious but there was a Treasury Enforcement Communications System alert on Cotterman based on prior sexual misconduct with a minor. A forensically trained agent wanted to look at the computer. Mr. Cotterman offered to help open the computer but was refused access to it. He then said there were multiple users of the laptop and he would have to get passwords from business associates. His laptop was held awaiting the passwords but Mr. Cotterman boarded a flight back to Mexico with a final destination of Australia.

The laptop was eventually opened and 378 images of child pornography were found. The District Court suppressed the images holding that there was too much time and space involved between seizing the computer and getting into it. The Ninth Circuit reversed but with a holding that reflects emerging thought processes related to personally used technology:

Still, the line we draw stops far short of “anything goes” at the border. The Government cannot simply seize property under its border search power and hold it for weeks, months, or years on a whim. Rather, we continue to scrutinize searches and seizures effectuated under the longstanding border search power on a case-by-case basis to determine whether the manner of the search and seizure was so egregious as to render it unreasonable.

The broad latitude of the border search prompted the 9th Circuit to accept the case for a rehearing en banc. The holding, has not (at the time of this writing) been published but the following is the key element of the holding:

The relevant inquiry, as always, is one of reasonableness. But that reasonableness determination must account for differences in property. Unlike searches involving a reassembled gas tank, or small hole in the bed of a pickup truck, which have minimal or no impact beyond the search itself—and little implication for an individual’s dignity and privacy interests—the exposure of confidential and personal information has permanence. It cannot be undone. Accordingly, the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property. . . . It is the potential unfettered dragnet effect that is troublesome.

There were strong dissents to this en banc hearing. The one probably most relevant to the issues in this paper comes from Justice Smith who contended that the majority was doubly wrong—first for requiring reasonable suspicion for the search and then for finding that the agents in Cotterman’s case had met that high standard.

These issues are sharpened as intelligence and law enforcement authorities seek to compile information to protect society. The concern for terrorism has driven a lot of that endeavor. Last year the ACLU released a report indicating that under the Obama Administration surveillance activities have risen sharply. For example, the report states that the Dept. of Justice used “pen register” and “trap and trace” techniques 23,535 times in 2009 and 37,616 times in 2011. In all, law enforcement made 1.3 million such requests in 2011.

During this time period, the number of people whose telephones were the subject of pen register and trap and trace surveillance more than tripled. In fact, more people were subjected to pen register and trap and trace surveillance in the past two years than in the entire previous decade. The number of authorizations to use these devices increased 361% and all without traditional warrant authorization.

Under current practices, this government surveillance activity cannot be directed solely at suspected terrorists and criminals and the result is that it can be directed at any of us. Increasingly, the government is engaged in warrantless surveillance that vacuums up sensitive information about innocent people. And this surveillance takes place in secret, with little or no oversight by the courts, by Congress, or by the public.

Using their power to collect massive amounts of private communications and data, agencies like the FBI and the National Security Agency (NSA) apply computer programs to draw links and make predictions about people’s behavior. Tracking people two, three, four steps removed from the original surveillance target, they build “communities of interest” and construct maps of our associations and activities.

With this sensitive data, the government can compile vast dossiers about innocent people. The data sits indefinitely in government databases, and the names of many innocent Americans may end up on inaccurate watch lists that affect whether we can fly on commercial airlines, whether we can renew our passports, whether we are called aside for “secondary screening” at airports and borders, and even whether we can open bank accounts.

However, it is also necessary to maintain a broad perspective—all such activities should not inspire conspiracy theories. ICE, for example is freeing sex slaves partly through software that identifies their geographic locations by synching financial transactions, phone records and other discordant data.ICE officials said recently. Typically, data mining incenses civil liberties advocates, but sifting through mounds of
personal information is helping U.S. law enforcement and human rights activists to convict participants in the $32 billion human trafficking trade. The FBI roots out criminals, terrorists and espionage agents utilizing these techniques. Customs and Border officials use accumulated data when allowing individuals to cross borders. The fundamental problem, however, was stated by Director of National Intelligence, James Clapper, on March 12, 2013:

“In some cases, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks.”

The World We Live In

The 16-20-something crowd may not appreciate how much the world has changed in such a very short order because it is their world—technology has always defined their lives, there have always been smart phones, Internet and social media. For the rest of us it has been a dizzying ride of only a couple of decades. However, we have come to appreciate the ease and comfort of the new technology, confident that we can manage our digital lives. We give limited consent to merchants and governments to collect certain information about us so that we can take advantage of new technology. Daniel Solov of The George Washington University School of Law describes this as privacy self-management. However, professor Solov goes on to explain why this is self-delusion. In a complex and increasingly digital world, it becomes infeasible for people to effectively self-manage their privacy.17

The reason for this is two-fold. First there is the obvious structural problem inherent in the myriad ways and reasons for collection of private data. There are simply too many entities that collect our information—mostly with our express or implied consent—for us to really keep track of where our information goes. Secondly, and more concerning, is the fact that once information is collected it may or may not be controlled against further dissemination. The digital ability to aggregate data makes it virtually impossible for us to weigh the costs and benefits of our consent to collection of private information against possible downstream uses.

At present there is little control over what private entities collect and what they do with the information they possess. We are comforted when we give our information to a business or other entity and see the legend on the relevant digital site “we do not provide or sell your private information.” However, the recent concern, both national and international, of the collection of metadata by the National Security Agency raises the question of what guarantees we have against disclosure of our information by and to the government.

Historically, when we thought of government collection of information the image that came to mind was that of a wiretap. However, in the current era this image is woefully inadequate. Today, online surveillance is less about capturing an ephemeral conversation than it is about aggregating a vast array of electronic information. Even the types of information that enjoy legal protections—health, financial and communications—are increasingly discoverable online. Compare this fact of modern life with the fundamental requirement that a democratic government owes to its people the protection of their private information and we have to consider whether our public institutions have been able to remain current with their protective responsibilities.

Experts in the field say that American technology has made the United States a surveillance superpower, allowing government the potential to access massive mountains of data being collected by the world’s leading communications, social media, and online storage companies. Then, too, the United States’ fiber optic infrastructure—responsible for just under a third of the world’s international Internet capacity, according to telecom research firm TeleGeography—allows it to act as a global postmaster, complete with the ability to peek at a big chunk of the world’s messages in transit.

“The sheer power of the U.S. infrastructure is that quite often data would be routed through the U.S. even if it didn’t make geographical sense,” Joss Wright, a researcher with the Oxford Internet Institute, said in a telephone interview. “The current status quo is a huge benefit to the U.S.”18

More than this, the government, in an effort to prevent the next Bradley Manning or Edward Snowden, or to stop the next terrorism attack, is seeking new ways to acquire and aggregate information that may be probative of the potentially dangerous anomaly. For example, in the months following the WikiLeaks revelations, the Defense Advanced Research Projects Agency (DARPA) – the U.S. military’s far-out tech arm – put out a number of requests for research on methods to detect suspicious behavior in large datasets. In addition, DARPA for some time has been


18. Id.
working with a number of organizations to investigate whether access to information in privately held data sources would measurably increase the government’s ability to deter terrorist activities. This is an entirely reasonable question.

If we consider the examples of the 9/11 hijackers we can construct a scenario in which, with government access to certain, publicly available information, we might have been able to prevent the attack. Two of the hijackers were known and known to be in the United States. They made airline reservations with two addresses, one of which was used by three additional hijackers. Various hijackers lived together, once two of them used the same frequent-flyer number, and they frequently used common telephone numbers. One was an out-of-status alien who had close contacts with five other hijackers. With access to the relevant data, none of which is protected by the Fourth Amendment, it might have made a difference on that fateful day.

Of course, what that means is the government would somehow have access to private information held in the private sector – often data that we might not want the government to have. The apartment rental agent has access to information regarding a person’s credit worthiness, former rentals, etc. The telephone company can pinpoint where a person was at the time of a phone call. In an era when data collection is an increasingly facile task, it logically becomes necessary that the production and use of that information should be subject to rigid controls – controls that were non-existent when collection capabilities began to feed on steroids.

Even if we agree that the government needs access to information of this nature to prevent harm, the question remains under what conditions this would be acceptable to the general public. It is abundantly clear that a suspicious public will be concerned about any prospect that the government should be solely responsible for oversight of any mechanisms that broadly sweep into government coffers information about its citizenry.

Therefore, one option might be that the information would remain under the control of the private entity while software strips personally identifying information (name, social security number, credit card numbers, etc.). This would be consistent with the vast majority of “wiretap” and other intelligence collection wherein a communications provider (as example) is provided with a warrant and directed to provide the requested information. In most such collection processes, the government does not have access to the data banks containing the information sought.

It should also be the case that the judiciary would have control over retrieval of personally identifying information, but even that would be subject to the question of what “standard” should be applied. Presumably, “probable cause” would be the standard, but probable cause for what. In criminal cases it is that a crime has been, is being or will be committed. In intelligence cases it is that the target is a “foreign power,” or an “agent” of a foreign power. These are standards decades old, and while they may be perfectly adequate for the modern age of technology, they at least should be examined for current validity.

Then, too, there is the realistic issue of an “emergency” situation and whether under what conditions, the privacy protections could be ignored.

These are extremely difficult issues to confront. They require legislation at a minimum, but legislation which has the considered input of intelligence and law enforcement agencies, of technologically advanced research organizations and of the privacy community. It should also be borne in mind that private industry will undoubtedly resist any legislation that does not constitutionally compel their cooperation.

Perhaps most importantly, we have to try to imagine the future of any privacy appliance measured against advancing technology. We have to bear in mind that we are witnessing technology advancing faster than we have been able to contemplate all of its meaning with respect to security and privacy. Any privacy appliance needs to be monitored as much by relevant technicians and/or scientists as by politicians, the privacy lobby or government watchdogs.

M. E. “Spike” Bowman, Esq., Capt., USN(Ret), a specialist in national security law and policy, served as the Deputy, National Counterintelligence Executive, part of the Office of the Director of National Intelligence. He previously served as Senior Research Fellow, National Defense University. Before that he served in the Senior Executive Service, Federal Bureau of Investigation as Senior Counsel, National Security Law, and as Director, Intelligence Issues Group, National Security Branch. He retired from the FBI in 2006. Prior to that he had an extensive Naval career which included assignments at the National Security Agency. Mr. Bowman has authored numerous articles on national security issues and is a frequent lecturer at conferences and universities both in the United States and abroad. He is a life member of AFIO and serves as Chairman of AFIO’s National Board of Directors.
Cyber-intruder sparks massive federal response — and debate over dealing with threats

By Ellen Nakashima, Published: December 8, 2011

The first sign of trouble was a mysterious signal emanating from deep within the U.S. military's classified computer network. Like a human spy, a piece of covert software in the supposedly secure system was "beaconing" — trying to send coded messages back to its creator.

An elite team working in a windowless room at the National Security Agency soon determined that a rogue program had infected a classified network, kept separate from the public Internet, that harbored some of the military's most important secrets, including battle plans used by commanders in Afghanistan and Iraq.

The government's top cyberwarriors couldn't immediately tell who created the program or why, although they would come to suspect the Russian intelligence service. Nor could they tell how long it had been there, but they soon deduced the ingeniously simple means of transmission, according to several current and former U.S. officials. The malicious software, or malware, caught a ride on an everyday thumb drive that allowed it to enter the secret system and begin looking for documents to steal. Then it spread by copying itself onto other thumb drives.

Pentagon officials consider the incident, discovered in October 2008, to be the most serious breach of the U.S. military's classified computer systems. The response, over the past three years, transformed the government's approach to cybersecurity, galvanizing the creation of a new military command charged with bolstering the military's computer defenses and preparing for eventual offensive operations. The efforts to neutralize the malware, through an operation code-named Buckshot Yankee, also demonstrated the importance of computer espionage in devising effective responses to cyberthreats.

But the breach and its aftermath also have opened a rare window into the legal concerns and bureaucratic tensions that affect military operations in an arena where the United States faces increasingly sophisticated threats. Like the running debates over the use of drones and other evolving military technologies, rapid advances in computing capability are forcing complex deliberations over the appropriate use of new tools and weapons.
This article, which contains previously undisclosed information on the extent of the infection, the nature of the response and the fractious policy debate it inspired, is based on interviews with two dozen current and former U.S. officials and others with knowledge of the operation. Many of them assert that while the military has a growing technical capacity to operate in cyberspace, it lacks authority to defend civilian networks effectively.

“The danger is not so much that cyber capabilities will be used without warning by some crazy general,” said Stewart A. Baker, a former NSA general counsel. “The real worry is they won’t be used at all because the generals don’t know what the rules are.”

A furious investigation

The malware that provoked Buckshot Yankee had circulated on the Internet for months without causing alarm, as just one threat among many. Then it showed up on the military computers of a NATO government in June 2008, according to Mikko Hypponen, chief research officer of a Finnish firm that analyzed the intruder.

He dubbed it “Agent.btz,” the next name in a sequence used at his company, F-Secure. “Agent.btz” was taken.

Four months later, in October 2008, NSA analysts discovered the malware on the Secret Internet Protocol Router Network, which the Defense and State departments use to transmit classified material but not the nation’s most sensitive information. Agent.btz also infected the Joint Worldwide Intelligence Communication System, which carries top-secret information to U.S. officials throughout the world.

Such networks are typically “air-gapped” — physically separated from the free-for-all of the Internet, with its countless varieties of malicious code, such as viruses and worms, created to steal information or damage systems. Officials had long been concerned with the unauthorized removal of classified material from secure networks; now malware had gotten in and was attempting to communicate to the broader Internet.

One likely scenario is that an American soldier, official or contractor in Afghanistan — where the largest number of infections occurred — went to an Internet cafe, used a thumb drive in an infected computer and then inserted the drive in a classified machine. “We knew fairly confidently that the mechanism had been somebody going to a kiosk and doing something they shouldn’t have as opposed to somebody who had been able to get inside the network,” one former official said.

Once a computer became infected, any thumb drive used on the machine acquired a copy of Agent.btz, ready for propagation to other computers, like bees carrying pollen from flower to flower. But to steal content, the malware had to communicate with a master computer for instructions on what files to remove and how to transmit them.

These signals, or beacons, were first spotted by a young analyst in the NSA’s Advanced Networks Operations (ANO) team, a group of mostly 20- and 30-something computing experts assembled in 2006 to hunt for suspicious activity on the government’s secure networks. Their office was a nondescript windowless room in Ops1, a boxy, low-rise building on the 660-acre campus of the NSA.

ANO’s operators are among 30,000 civilian and military personnel at NSA, whose main mission is to collect foreign communications intelligence on enemies abroad. The agency is forbidden to gather intelligence on Americans or on U.S. soil without special authorization from a court whose proceedings are largely secret.

NSA, whose employees hold 800 PhDs in mathematics, science and engineering, is based at Fort Meade, an
Army base between Baltimore and Washington that has the world’s largest collection of supercomputers as well as its own police force and silicon-chip plant.

The ANO operators determined that the breach was serious after a few days of furious investigation. On the afternoon of Friday, Oct. 24, Richard C. Schaeffer Jr., then the NSA’s top computer systems protection officer, was in an agency briefing with President George W. Bush, who was making his last visit to the NSA before leaving office. An aide handed Schaeffer a note alerting him to the breach.

At 4:30 p.m., Schaeffer entered the office of Gen. Keith Alexander, the NSA director and a veteran military intelligence officer.

Alexander recalled that Schaeffer minced no words. “We’ve got a problem,” he said.

Permanent slumber

That evening, NSA officials briefed top levels of the U.S. government: the chairman of the Joint Chiefs of Staff, the deputy defense secretary and senior congressional leaders, telling them about the incident.

Working through the night, the ANO operators pursued a potential fix. Since Agent.btz was beaconing out in search of instructions, perhaps they could devise a way to order the malware to shut itself down. The next morning, in a room strewn with empty pizza boxes and soda cans, they sketched out their plan on a white board. But before it could be put into action, the NSA team had to make sure it would not affect the performance of other software, including the programs that battlefield commanders use for intelligence and communications. They needed to run a test.

“Our objective,” recalled Schaeffer, “was first, do no harm.”

That afternoon, the team members loaded a computer server into a truck and drove it to a nearby office of the Defense Information Systems Agency, which operates the department’s long-haul telecommunications and satellite networks.

At 2:30 p.m. they activated a program designed to recognize the beaconing of Agent.btz and respond. Soon after, the malware on the test server fell into permanent slumber.

Devising the technical remedy was only the first step. Defeating the threat required neutralizing Agent.btz everywhere it had spread on government networks, a grueling process that involved isolating individual computers, taking them offline, cleaning them, and reformatting hard drives.

A key player in Buckshot Yankee was NSA’s Tailored Access Operations (TAO), a secretive unit dating to the early 1990s that specialized in intelligence operations overseas focused on gathering sensitive technical information. These specialists ventured outside the military’s networks to look for Agent.btz in a process called “exploitation” or electronic spying.

The TAO identified new variants of the malware and helped network defenders prepare to neutralize them before they infected military computers.

“It’s the ability to look outside our wire,” said one military official.
Officials debated whether to use offensive tools to neutralize the malware on non-military networks, including those in other countries. The military’s offensive cyber unit, Joint Functional Component Command — Network Warfare, proposed some options for doing so.

Senior officials rejected them on the grounds that Agent.btz appeared to be an act of espionage, not an outright attack, and didn’t justify such an aggressive response, according to those familiar with the conversations.

As the NSA worked to neutralize Agent.btz on its government computers, Strategic Command, which oversees deterrence strategy for nuclear weapons, space and cyberspace, raised the military’s information security threat level. A few weeks later, in November, an order went out banning the use of thumb drives across the Defense Department worldwide. It was the most controversial order of the operation.

Agent.btz had spread widely among military computers around the world, especially in Iraq and Afghanistan, creating the potential for major losses of intelligence. Yet the ban generated backlash among officers in the field, many of whom relied on the drives to download combat imagery or share after-action reports.

The NSA and the military investigated for months how the infection occurred. They retrieved thousands of thumb drives, many of which were infected. Much energy was spent trying to find “Patient Zero,” officials said. “It turned out to be too complicated,” said one. “We could never bring it down to as clear as … ‘that’s the thumb drive.’”

The rate of new infections finally subsided in early 2009. Officials say no evidence emerged that Agent.btz succeeded in communicating with a master computer or in putting secret documents in enemy hands. The ban on thumb drives has been partially lifted because other security measures have been put in place.

‘A great catalyst’

Buckshot Yankee bolstered the argument for creating Cyber Command, a new unit designed to protect the military’s computer and communications systems. It gave NSA Director Alexander the platform to press the case, advocated by others, that the new command should be able to use the NSA’s capabilities to obtain foreign intelligence to defend the military’s systems.

“It was a great catalyst,” said Alexander, although the effort later faced questions about whether the head of the largest and most secretive intelligence agency should also lead the new organization.

The new organization, which has a staff of 750 and a budget of $155 million, brings together the Joint Task Force-Global Network Operations, which carried out the bulk of the cleanup work under Buckshot Yankee, and the Network Warfare unit, the military’s offensive cyber arm. It began full operations on Oct. 31, 2010, with Alexander as its head.

But the creation of Cyber Command did not resolve several key debates over the national response to cyberthreats. Agent.btz provoked renewed discussion among senior officials at the White House and key departments about how to best protect critical private-sector networks.

Some officials argued that the military was better equipped than the Department of Homeland Security to respond to a major destructive attack on a power grid or other critical system, but others disagreed.

“Cyber Command and [Strategic Command] were asking for way too much authority” by seeking permission to
take “unilateral action . . . inside the United States,” said Gen. James F. Cartwright Jr., who retired as vice chairman of the Joint Chiefs in August.

Officials also debated how aggressive military commanders can be in defending their computer systems.

“You have the right of self-defense, but you don’t know how far you can carry it and under what circumstances, and in what places,” Cartwright said. “So for a commander who’s out there in a very ambiguous world looking for guidance, if somebody attacks them, are they supposed to run? Can they respond?”

Questions over the role of offense in cybersecurity deterrence began in the 1990s, if not earlier, said Martin Libicki, a Rand Corp. cyberwarfare expert. One reason it is so difficult to craft rules, he said, is the tendency to cast cyberwar as “good, old-fashioned war in yet another domain.” Unlike conventional and nuclear warfare, cyberattacks generally are enabled only by flaws in the target system, he said.

Another reason it is so difficult, said James A. Lewis, a senior fellow at the Center for Strategic and International Studies, is the overlap between cybersecurity operations and the classified world of intelligence.

“The link to espionage is where the nuclear precedent breaks down and makes cyber closer to covert operations,” Lewis said.

By the summer of 2009, Pentagon officials had begun work on a set of rules of engagement, part of a broader cyberdefense effort called Operation Gladiator Phoenix. They drafted an “execute order” under which the Strategic and Cyber commands could direct the operations and defense of military networks anywhere in the world. Initially, the directive applied to critical privately owned computer systems in the United States.

Several conditions had to be met, according to a military official familiar with the draft order. The provocation had to be hostile and directed at the United States, its critical infrastructure or citizens. It had to present the imminent likelihood of death, serious injury or damage that threatened national or economic security. The response had to be coordinated with affected government agencies and combatant commanders. And it had to be limited to actions necessary to stop the attack, while minimizing impacts on non-military computers.

“Say someone launched an attack on the U.S. from a known Chinese army computer — a known hostile computer,” the official said. “You could maybe disable the computer, but you’re not talking about making it explode and killing somebody.”

Turf battles

But the effort to create such comprehensive rules of engagement foundered, said current and former officials with direct knowledge of the policy debate.

The Justice Department feared setting a legal precedent for military action in domestic networks. The CIA resisted letting the military infringe on its foreign turf. The State Department worried the military would accidentally disrupt a server in a friendly country without seeking consent, undermining future cooperation. The Department of Homeland Security, meanwhile, worked to keep its lead role in securing the nation against cyberthreats.

The debate bogged down over how far the military could go to parry attacks, which can be routed from server to server, sometimes in multiple countries. “Could you go only to the first [server] you trace back to? Could you
go all the way to the first point at which the attack emanated from? Those were the questions that were still being negotiated,” said a former U.S. official.

The questions were even more vexing when it came to potentially combating an attack launched from servers within the United States. The military has no authority to act in cyberspace when the networks are domestic — unless the operation is on its own systems.

In October 2010, Pentagon officials signed an agreement with the Department of Homeland Security pledging to work to enhance the nation’s cybersecurity. But in speeches, Alexander, the head of Cyber Command, has suggested that more needs to be done.

“Right now, my mission as commander of U.S. Cyber Command is to defend the military networks,” he said in an April speech in Rhode Island. “I do not have the authority to look at what’s going on in other government sectors, nor what would happen in critical infrastructure. That right now falls to DHS. It also means that I can’t stop it, or at network speed … see what’s happening to it. What we do believe, though, is that that needs to be accounted for. We have to have a way to protect our critical infrastructure.”

Homeland Security Secretary Janet Napolitano, in a speech in California that same month, made her preference clear. “At DHS, we believe cyberspace is fundamentally a civilian space.”

The execute order was signed in February. The standing rules of engagement limit the military to the defense of its own networks and do not allow it to go outside them without special permission from the president.

The next vulnerability?

Almost from the beginning, U.S. officials suspected that Russia’s spy service created Agent.btz to steal military secrets. In late 2008, Russia issued a denunciation of the allegation, calling it “groundless” and “irresponsible.”

Former officials say there is evidence of a Russian role in developing the malware, but some doubt whether the spy service created Agent.btz to infiltrate U.S. military computers.

Some say it could have been a product of Russia’s sophisticated mafia, with its extensive computer expertise, to collect all sorts of protected records worth stealing — or selling to the highest bidder. Or there could have been Russian involvement in one phase of the malware’s development before it was adapted by others. Others say they have no doubt that it was intentionally aimed at the Defense Department. New versions of Agent.btz continue to appear, years after it was discovered.

What is clear is that Agent.btz revealed weaknesses in crucial U.S. government computer networks — vulnerabilities based on the weakest link in the security chain: human beings. The development of new defenses did not prevent the transfer of massive amounts of information from one classified network to the anti-secrecy group WikiLeaks, an act that the government charges was carried out by an Army intelligence analyst.

NSA analysts know how to neutralize Agent.btz and its variants, but no one knows when the next vulnerability will be discovered or what kind of intrusion might ensue.

Richard “Dickie” George, who was the NSA information assurance technical director until his retirement this year, said that in the early days of Operation Buckshot Yankee, a four-star general asked when the danger from Agent.btz would pass and heightened security measures could end.
"We had to break the news to him," George recalled, "that this is never going to be over."

*Staff researcher Julie Tate contributed to this report.*
Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See United States v. Detroit Timber & Lumber Co., 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

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.
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) (Flaum, 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
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 Po-

tioning System (GPS) device to monitor a vehicle's move-
ments 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\(^1\) to the under-
side of the vehicle that respondent drove, the law enfor-
sement officers in this case engaged in conduct that might
have provided grounds in 1791 for a suit for trespass to
chattels.\(^2\) And for this reason, the Court concludes,
the installation and use of the GPS device constituted

\(^1\)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) (here-
inafter Prosser & Keeton). Here, there was no actual damage to the
vehicle to which the GPS device was attached.
ALITO, J., concurring in judgment

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
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 Kyllo 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 “hous[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
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

\^See, e.g., Cal. Family Code Ann. §760 (West 2004).
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, 1866, 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 *Katz* overruled *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. 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. 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.
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 situ-
ated to gauge changing public attitudes, to draw detailed
lines, and to balance privacy and public safety in a com-
prehensive way.

To date, however, Congress and most States have not
enacted statutes regulating the use of GPS tracking tech-
nology 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 rea-
sonable 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 cata-
logue every single movement of an individual’s car for
a very long period. In this case, for four weeks, law en-
forcement agents tracked every movement that respond-
ent 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., \textit{United States v. Gerber}, 994 F. 2d 1556, 1559–1560 (CA11 1993); \textit{United States v. Burke}, 517 F. 2d 377, 386–387 (CA2 1975). Because it was not raised, that question is not before us.
FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part III

The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity
Executive Order 13636 of February 12, 2013

Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation’s critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the “Secretary”), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of
Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 ( Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National
Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").
(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification
of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) “Agency” means any authority of the United States that is an “agency” under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) “Critical Infrastructure Partnership Advisory Council” means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) “Fair Information Practice Principles” means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) “Independent regulatory agency” has the meaning given the term in 44 U.S.C. 3502(5).

(e) “Sector Coordinating Council” means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) “Sector-Specific Agency” has the meaning given the term in Presidential Policy Directive–21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater
extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersedes measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
February 12, 2013.
PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure - including assets, networks, and systems - that are vital to public confidence and the Nation's safety, prosperity, and well-being.

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.
Policy

It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.

The Federal Government shall also engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States on which the Nation depends.

U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.

Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:

1) Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure shall be addressed in the plans and execution of the requirements in the National Continuity Policy.

Federal departments and agencies shall implement this directive in a manner consistent with applicable law, Presidential directives, and Federal regulations, including those protecting privacy, civil rights, and civil liberties. In addition, Federal departments and agencies shall protect all information associated with carrying out this directive consistent with applicable legal authorities and policies.

Roles and Responsibilities

Effective implementation of this directive requires a national unity of effort pursuant to strategic guidance from the Secretary of Homeland Security. That national effort must include expertise and day-to-day engagement from the Sector-Specific Agencies (SSAs) as well as the specialized or support capabilities from other Federal departments and agencies, and
strong collaboration with critical infrastructure owners and operators and SLTT entities. Although the roles and responsibilities identified in this directive are directed at Federal departments and agencies, effective partnerships with critical infrastructure owners and operators and SLTT entities are imperative to strengthen the security and resilience of the Nation's critical infrastructure.

Secretary of Homeland Security
The Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. In carrying out the responsibilities assigned in the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure.

Additional roles and responsibilities for the Secretary of Homeland Security include:

1) Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with SSAs and other Federal departments and agencies;
2) Maintain national critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure;
3) In coordination with SSAs and other Federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure;
4) Conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators;
5) Coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities;
6) Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;
7) Coordinate with and utilize the expertise of SSAs and other appropriate Federal departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies; and
8) Report annually on the status of national critical infrastructure efforts as required by statute.

Sector-Specific Agencies
Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified Sector-Specific Agency that has institutional knowledge and specialized expertise about the sector. Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, SSAs shall carry out the following roles and responsibilities for their respective sectors:

1) As part of the broader national effort to strengthen the security and resilience of critical infrastructure, coordinate with the Department of Homeland Security (DHS) and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate, to implement this directive;

2) Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities;

3) Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;

4) Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and

5) Support the Secretary of Homeland Security's statutorily required reporting requirements by providing on an annual basis sector-specific critical infrastructure information.

Additional Federal Responsibilities
The following departments and agencies have specialized or support functions related to critical infrastructure security and resilience that shall be carried out by, or along with, other Federal departments and agencies and independent regulatory agencies, as appropriate.

1) The Department of State, in coordination with DHS, SSAs, and other Federal departments and agencies, shall engage foreign governments and international organizations to strengthen the security and resilience of critical infrastructure located outside the United States and to facilitate the overall exchange of best practices and lessons learned for promoting the security and resilience of critical infrastructure on which the Nation depends.

2) The Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), shall lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors. DOJ shall investigate, disrupt, prosecute, and otherwise reduce foreign intelligence, terrorist, and other threats to, and actual or attempted attacks on, or sabotage of, the Nation's critical infrastructure. The FBI also conducts domestic collection, analysis, and dissemination of cyber threat information, and shall be responsible for the operation of the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, the Intelligence Community (IC), the Department of
Defense (DOD), and other agencies as appropriate. The Attorney General and the Secretary of Homeland Security shall collaborate to carry out their respective critical infrastructure missions.

3) The Department of the Interior, in collaboration with the SSA for the Government Facilities Sector, shall identify, prioritize, and coordinate the security and resilience efforts for national monuments and icons and incorporate measures to reduce risk to these critical assets, while also promoting their use and enjoyment.

4) The Department of Commerce (DOC), in collaboration with DHS and other relevant Federal departments and agencies, shall engage private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems, and promote the development of other efforts related to critical infrastructure to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.

5) The IC, led by the Director of National Intelligence (DNI), shall use applicable authorities and coordination mechanisms to provide, as appropriate, intelligence assessments regarding threats to critical infrastructure and coordinate on intelligence and other sensitive or proprietary information related to critical infrastructure. In addition, information security policies, directives, standards, and guidelines for safeguarding national security systems shall be overseen as directed by the President, applicable law, and in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

6) The General Services Administration, in consultation with DOD, DHS, and other departments and agencies as appropriate, shall provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.

7) The Nuclear Regulatory Commission (NRC) is to oversee its licensees' protection of commercial nuclear power reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings, and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste. The NRC is to collaborate, to the extent possible, with DHS, DOJ, the Department of Energy, the Environmental Protection Agency, and other Federal departments and agencies, as appropriate, on strengthening critical infrastructure security and resilience.

8) The Federal Communications Commission, to the extent permitted by law, is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends.
9) Federal departments and agencies shall provide timely information to the Secretary of Homeland Security and the national critical infrastructure centers necessary to support cross-sector analysis and inform the situational awareness capability for critical infrastructure.

Three Strategic Imperatives

1) Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience

An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by the expertise, experience, capabilities, and responsibilities of the SSAs, other Federal departments and agencies with critical infrastructure roles, SLTT entities, and critical infrastructure owners and operators.

During the past decade, new programs and initiatives have been established to address specific infrastructure issues, and priorities have shifted and expanded. As a result, Federal functions related to critical infrastructure security and resilience shall be clarified and refined to establish baseline capabilities that will reflect this evolution of knowledge, to define relevant Federal program functions, and to facilitate collaboration and information exchange between and among the Federal Government, critical infrastructure owners and operators, and SLTT entities.

As part of this refined structure, there shall be two national critical infrastructure centers operated by DHS - one for physical infrastructure and another for cyber infrastructure. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure. Just as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities. Accordingly, an integration and analysis function (further developed in Strategic Imperative 3) shall be implemented between these two national centers.

The success of these national centers, including the integration and analysis function, is dependent on the quality and timeliness of the information and intelligence they receive from the SSAs and other Federal departments and agencies, as well as from critical infrastructure owners and operators and SLTT entities.

These national centers shall not impede the ability of the heads of Federal departments and agencies to carry out or perform their responsibilities for national defense, criminal, counterintelligence, counterterrorism, or investigative activities.

2) Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government

A secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical
infrastructure owners and operators. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents. The goal is to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.

Greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties. Federal departments and agencies shall ensure that all existing privacy principles, policies, and procedures are implemented consistent with applicable law and policy and shall include senior agency officials for privacy in their efforts to govern and oversee information sharing properly.

3) Implement an Integration and Analysis Function to Inform Planning and Operational Decisions Regarding Critical Infrastructure

The third strategic imperative builds on the first two and calls for the implementation of an integration and analysis function for critical infrastructure that includes operational and strategic analysis on incidents, threats, and emerging risks. It shall reside at the intersection of the two national centers as identified in Strategic Imperative 1, and it shall include the capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to:

- Aid in prioritizing assets and managing risks to critical infrastructure;
- Anticipate interdependencies and cascading impacts;
- Recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident; and
- Support incident management and restoration efforts related to critical infrastructure.

This function shall not replicate the analysis function of the IC or the National Counterterrorism Center, nor shall it involve intelligence collection activities. The IC, DOD, DOJ, DHS, and other Federal departments and agencies with relevant intelligence or information shall, however, inform this integration and analysis capability regarding the Nation's critical infrastructure by providing relevant, timely, and appropriate information to the national centers. This function shall also use information and intelligence provided by other critical infrastructure partners, including SLTT and nongovernmental analytic entities.

Finally, this integration and analysis function shall support DHS's ability to maintain and share, as a common Federal service, a near real-time situational awareness capability for critical infrastructure that includes actionable information about imminent threats, significant trends, and awareness of incidents that may affect critical infrastructure.

Innovation and Research and Development
The Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy (OSTP), the SSAs, DOC, and other Federal departments and agencies, shall provide input to align those Federal and Federally-funded research and development (R&D) activities that seek to strengthen the security and resilience of the Nation's critical infrastructure, including:

1) Promoting R&D to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;
2) Enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, as well as cascading effects on other sectors;
3) Facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and
4) Prioritizing efforts to support the strategic guidance issued by the Secretary of Homeland Security.

Implementation of the Directive

The Secretary of Homeland Security shall take the following actions as part of the implementation of this directive.

1) Critical Infrastructure Security and Resilience Functional Relationships. Within 120 days of the date of this directive, the Secretary of Homeland Security shall develop a description of the functional relationships within DHS and across the Federal Government related to critical infrastructure security and resilience. It should include the roles and functions of the two national critical infrastructure centers and a discussion of the analysis and integration function. When complete, it should serve as a roadmap for critical infrastructure owners and operators and SLTT entities to navigate the Federal Government's functions and primary points of contact assigned to those functions for critical infrastructure security and resilience against both physical and cyber threats. The Secretary shall coordinate this effort with the SSAs and other relevant Federal departments and agencies. The Secretary shall provide the description to the President through the Assistant to the President for Homeland Security and Counterterrorism.

2) Evaluation of the Existing Public-Private Partnership Model. Within 150 days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators, shall conduct an analysis of the existing public-private partnership model and recommend options for improving the effectiveness of the partnership in both the physical and cyber space. The evaluation shall consider options to streamline processes for collaboration and exchange of information and to minimize duplication of effort. Furthermore, the analysis shall consider how the model can be flexible and adaptable to meet the unique needs of individual sectors while providing a focused, disciplined, and effective approach for the Federal Government to coordinate with the critical infrastructure owners and operators and with SLTT governments. The evaluation shall result in recommendations to enhance partnerships to be approved for implementation through the
processes established in the Organization of the National Security Council System directive.

3) **Identification of Baseline Data and Systems Requirements for the Federal Government to Enable Efficient Information Exchange.** Within 180 days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs and other Federal departments and agencies, shall convene a team of experts to identify baseline data and systems requirements to enable the efficient exchange of information and intelligence relevant to strengthening the security and resilience of critical infrastructure. The experts should include representatives from those entities that routinely possess information important to critical infrastructure security and resilience; those that determine and manage information technology systems used to exchange information; and those responsible for the security of information being exchanged. Interoperability with critical infrastructure partners; identification of key data and the information requirements of key Federal, SUT, and private sector entities; availability, accessibility, and formats of data; the ability to exchange various classifications of information; and the security of those systems to be used; and appropriate protections for individual privacy and civil liberties should be included in the analysis. The analysis should result in baseline requirements for sharing of data and interoperability of systems to enable the timely exchange of data and information to secure critical infrastructure and make it more resilient. The Secretary shall provide that analysis to the President through the Assistant to the President for Homeland Security and Counterterrorism.

4) **Development of a Situational Awareness Capability for Critical Infrastructure.** Within 240 days of the date of this directive, the Secretary of Homeland Security shall demonstrate a near real-time situational awareness capability for critical infrastructure that includes threat streams and all-hazards information as well as vulnerabilities; provides the status of critical infrastructure and potential cascading effects; supports decision making; and disseminates critical information that may be needed to save or sustain lives, mitigate damage, or reduce further degradation of a critical infrastructure capability throughout an incident. This capability should be available for and cover physical and cyber elements of critical infrastructure, and enable an integration of information as necessitated by the incident.

5) **Update to National Infrastructure Protection Plan.** Within 240 days of the date of this directive, the Secretary of Homeland Security shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a successor to the National Infrastructure Protection Plan to address the implementation of this directive, the requirements of Title II of the Homeland Security Act of 2002 as amended, and alignment with the National Preparedness Goal and System required by PPD-8. The plan shall include the identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure; the methods to be used to prioritize critical infrastructure; the protocols to be used to synchronize communication and actions within the Federal Government; and a metrics and analysis process to be used to measure the Nation's ability to manage and reduce risks to
critical infrastructure. The updated plan shall also reflect the identified functional relationships within DHS and across the Federal Government and the updates to the public-private partnership model. Finally, the plan should consider sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems. The Secretary shall coordinate this effort with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators.

6) National Critical Infrastructure Security and Resilience R&D Plan. Within 2 years of the date of this directive, the Secretary of Homeland Security, in coordination with the OSTP, the SSAs, DOC, and other Federal departments and agencies, shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a National Critical Infrastructure Security and Resilience R&D Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. The plan should be issued every 4 years after its initial delivery, with interim updates as needed.

Policy coordination, dispute resolution, and periodic in-progress reviews for the implementation of this directive shall be carried out consistent with PPD-1, including the use of Interagency Policy Committees coordinated by the National Security Staff.

Nothing in this directive alters, supersedes, or impedes the authorities of Federal departments and agencies, including independent regulatory agencies, to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives, including, but not limited to, the designation of critical infrastructure under such authorities.

This directive revokes Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, issued December 17, 2003. Plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

**Designated Critical Infrastructure Sectors and Sector-Specific Agencies**

This directive identifies 16 critical infrastructure sectors and designates associated Federal SSAs. In some cases co-SSAs are designated where those departments share the roles and responsibilities of the SSA. The Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors and shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated SSA for that sector. The sectors and SSAs are as follows:

- **Chemical**:
  - Sector-Specific Agency: Department of Homeland Security

- **Commercial Facilities**:
  - Sector-Specific Agency: Department of Homeland Security
Communications:
Sector-Specific Agency: Department of Homeland Security

Critical Manufacturing:
Sector-Specific Agency: Department of Homeland Security

Dams:
Sector-Specific Agency: Department of Homeland Security

Defense Industrial Base:
Sector-Specific Agency: Department of Defense

Emergency Services:
Sector-Specific Agency: Department of Homeland Security

Energy:
Sector-Specific Agency: Department of Energy

Financial Services:
Sector-Specific Agency: Department of the Treasury

Food and Agriculture:
Co-Sector-Specific Agencies: U.S. Department of Agriculture and Department of Health and Human Services

Government Facilities:
Co-Sector-Specific Agencies: Department of Homeland Security and General Services Administration

Healthcare and Public Health:
Sector-Specific Agency: Department of Health and Human Services

Information Technology:
Sector-Specific Agency: Department of Homeland Security

Nuclear Reactors, Materials, and Waste:
Sector-Specific Agency: Department of Homeland Security

Transportation Systems:
Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation

Water and Wastewater Systems:
Sector-Specific Agency: Environmental Protection Agency

Definitions

For purposes of this directive:

The term "all hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

The term "collaboration" means the process of working together to achieve shared goals.
The terms "coordinate" and "in coordination with" mean a consensus decision-making process in which the named coordinating department or agency is responsible for working with the affected departments and agencies to achieve consensus and a consistent course of action.

The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely 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.

The term "Federal departments and agencies" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

The term "national essential functions" means that subset of Government functions that are necessary to lead and sustain the Nation during a catastrophic emergency.

The term "primary mission essential functions" means those Government functions that must be performed in order to support or implement the performance of the national essential functions before, during, and in the aftermath of an emergency.

The term "national security systems" has the meaning given to it in the Federal Information Security Management Act of 2002 (44 U.S.C. 3542(b)).

The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

The term "Sector-Specific Agency" (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

The terms "secure" and "security" refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

# # #
LEGALITY OF INTRUSION-DETECTION SYSTEM TO PROTECT UNCLASSIFIED COMPUTER NETWORKS IN THE EXECUTIVE BRANCH

Operation of the EINSTEIN 2.0 intrusion-detection system complies with the Fourth Amendment to the Constitution, title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Foreign Intelligence Surveillance Act, the Stored Communications Act, and the pen register and trap and trace provisions of chapter 206 of title 18, United States Code, provided that certain log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system. Operation of the EINSTEIN 2.0 system also does not run afoul of state wiretapping or communications privacy laws.

August 14, 2009

MEMORANDUM OPINION FOR AN ASSOCIATE DEPUTY ATTORNEY GENERAL


We have assumed for purposes of our analysis that computer users generally have a legitimate expectation of privacy in the content of Internet communications (such as an e-mail) while it is in transmission over the Internet. See, e.g., United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (analogizing expectation of email user in privacy of email to expectation of individuals communicating by regular mail); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (sender of an email generally “enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant”); see

---

1 Computer users do not have an objectively reasonable expectation of privacy in addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user. See Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 904-05 (9th Cir. 2008); United States v. Forrester, 512 F.3d 500, 510-11 (9th Cir. 2008); cf. Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies).
also Quon, 529 F.3d at 905 ("[U]sers do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider."). Even given this assumption, however, we believe the deployment, testing, and use of EINSTEIN 2.0 technology complies with the Fourth Amendment where each agency participating in the program consistently adopts, implements, and enforces the model log-on banner or model computer-user agreements described in this Office’s prior opinion, or their substantial equivalents. See EINSTEIN 2.0 Opinion at 5-6.

First, we conclude that the adoption, implementation, and enforcement of model log-on banners or model computer-user agreements eliminates federal employees’ reasonable expectation of privacy in their uses of Government-owned information systems with respect to the lawful government purpose of protecting federal systems against network intrusions and exploitations. We therefore do not believe that the operation of intrusion-detection sensors as part of the EINSTEIN 2.0 program constitutes a “search” for Fourth Amendment purposes. See Minnesota v. Carter, 525 U.S. 83, 88 (1998). Whether a Government employee has a legitimate expectation of privacy in his use of governmental property at work in particular circumstances is determined by “[t]he operational realities of the workplace,” and “by virtue of actual office practices and procedures, or by legitimate regulation.” O’Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality); see United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (“[O]ffice practices, procedures, or regulations may reduce legitimate privacy expectations.”). The existence of an expectation of privacy, moreover, may depend on the nature of the intrusion at issue. See O’Connor, 480 U.S. at 717-18 (plurality) (suggesting that a government employee’s expectation of privacy might be unreasonable “when an intrusion is by a supervisor” but reasonable when the intrusion is by a law enforcement official). The model banner and model computer-user agreement discussed in our prior opinion are at least as robust as—and we think stronger than—similar materials that courts have held eliminated a legitimate government employee expectation of privacy in the content of Internet communications sent over government systems. See, e.g., Simons, 206 F.3d at 398 (finding no legitimate expectation of privacy in light of computer-use policy expressly noting that government agency would “audit, inspect, and/or monitor” employees’ use of the Internet, “including all file transfers, all websites visited, and all e-mail messages, ‘as deemed appropriate’” (quoting policy); United States v. Angevine, 281 F.3d 1130, 1132-33 (10th Cir. 2002) (finding no legitimate expectation of privacy in light of computer-use policy stating that university “reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically” and has “a right of access to the contents of stored computing information at any time for any purpose which it has a legitimate need to know”’ (quoting policy); United States v. Thorn, 375 F.3d 679, 682 (8th Cir. 2004), vacated on other grounds, 543 U.S. 1112 (2005) (finding no legitimate expectation of privacy in light of computer-use policy warning that employees “do not have any personal privacy rights regarding their use of [the employing agency’s] information systems and technology,” and that “[a]n employee’s use of [the agency’s] information systems and technology indicates that the employee understands and consents to [the agency’s] right to inspect and audit all such use as described in this policy”) (quoting policy). We therefore believe that the adoption, implementation, and enforcement of the language in those model materials, or their substantial equivalents, by agencies participating in the EINSTEIN 2.0 program will eliminate federal employees’ legitimate expectations of privacy in their uses of
Government-owned information systems with respect to the lawful government purpose of protecting federal systems against network intrusions and exploitations.\(^2\)

We also believe that individuals in the private sector who communicate directly with federal employees of agencies participating in the EINSTEIN 2.0 program through Government-owned information systems do not have a legitimate expectation of privacy in the content of those communications provided that model log-on banners or agreements are adopted and implemented by the agency. The Supreme Court has repeatedly held that where a person "reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and that if occurs the Fourth Amendment does not prohibit governmental use of that information." \textit{United States v. Jacobsen}, 466 U.S. 109, 117 (1984); see also \textit{United States v. Miller}, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); \textit{SEC v. Jerry T. O'Brien, Inc.}, 467 U.S. 735, 743 (1984) ("[W]hen a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."); \textit{Smith}, 442 U.S. at 743-44 ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). We believe this principle also applies to a person who emails a federal employee at the employee’s personal email account when that employee accesses his or her personal email account through a Government-owned information system, when the consent procedures described above are followed. By clicking through the model log-on banner or agreeing to the terms of the model computer-user agreement, a federal employee gives \textit{ex ante} permission to the Government to intercept, monitor, and search "any communications" and "any data" transiting or stored on a Government-owned information system for any "lawful purpose," including the purpose of protecting federal computer systems against malicious network activity. Therefore, an individual who communicates with a federal employee who has agreed to permit the Government to intercept, monitor, and search any personal use of the employee’s Government-owned information systems has no Fourth Amendment right against the Government activity of protecting federal computer systems against malicious network activity, as the employee has consented to that activity. \textit{See Jerry T. O'Brien, Inc.}, 467 U.S. at 743; \textit{Jacobsen}, 466 U.S. at 117; \textit{Miller}, 425 U.S. at 443.

Under Supreme Court precedent, this principle applies even where, for example, the sender of an email to an employee’s personal, Web-based email account (such as Gmail or Hotmail) does not know of the recipient’s status as a federal employee or does not anticipate that the employee might read, on a federal Government system, an email sent to a personal email account at work or that the employee has agreed to Government monitoring of his communications on that system. A person communicating with another assumes the risk that the person has agreed to permit the Government to monitor the contents of that communication. \textit{See},

\(^2\) The use of log-on banners or computer-user agreements may not be sufficient to eliminate an employee’s legitimate expectation of privacy if the statements and actions of agency officials contradict these materials. \textit{See Quon}, 529 F.3d at 906-07. Management officials of agencies participating in the EINSTEIN 2.0 program therefore should ensure that agency practices are consistent with the statements in the model materials.
e.g., *United States v. White*, 401 U.S. 745, 749-51 (1971) (plurality opinion) (no Fourth Amendment protection against government monitoring of communications through transmitter worn by undercover operative); *Hoffa v. United States*, 385 U.S. 293, 300-03 (1966) (information disclosed to individual who turns out to be a government informant is not protected by the Fourth Amendment); *Lopez v. United States*, 373 U.S. 427, 439 (1963) (same); cf. *Rathbun v. United States*, 355 U.S. 107, 111 (1957) ("Each party to a telephone conversation takes the risk that the other party may have an extension telephone and may allow another to overhear the conversation. When such takes place there has been no violation of any privacy of which the parties may complain."). Accordingly, when an employee agrees to let the Government intercept, monitor, and search any communication or data sent, received, or stored by a Government-owned information system, the Government's interception of the employee's Internet communications with individuals outside of the relevant agency through a Government-owned information system does not infringe upon any legitimate expectation of privacy of the parties to that communication.

We also think that, under the Court's precedents, an individual who submits information through the Internet to a federal agency participating in the EINSTEIN 2.0 program does not have a legitimate expectation of privacy for Fourth Amendment purposes in the contents of the information that he transmits directly to the participating agency. An individual has no expectation of privacy in communications he makes to a known representative of the Government. See *United States v. Caceres*, 440 U.S. 741, 750-51 (1979) (individual has no reasonable expectation of privacy in communications with IRS agent made in the course of an audit). Further, as just discussed, an individual who communicates information to another individual who turns out to be an undercover agent of the Government has no legitimate expectation of privacy in the content of that information. It follows a fortiori that where an individual is communicating directly with a declared agent of the Government, the individual does not have a legitimate expectation that his communication would not be monitored or acquired by the Government.

Second, even if EINSTEIN 2.0 operations were to constitute a "search" under the Fourth Amendment, we believe that those operations would be consistent with the Amendment's "central requirement" that all searches be reasonable. *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (internal quotation marks omitted). As discussed in the prior opinion of this Office, the Government has a lawful, work-related purpose for the use of EINSTEIN 2.0's intrusion-detection system that brings the EINSTEIN 2.0 program within the "special needs" exception to the Fourth Amendment's warrant and probable cause requirements. See *O'Connor*, 480 U.S. at 720 (plurality); see also *Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665-66 (1989) (warrant and probable cause provisions of the Fourth Amendment are inapplicable to a search that "serves special governmental needs, beyond the normal need for law enforcement"); *Griffin v. Wisconsin*, 483 U.S. 868, 872-73 (1987) (special needs doctrine applies in circumstances that make the "warrant and probable cause requirement impracticable"); *United States v. Heckenkamp*, 482 F.3d 1142, 1148 (9th Cir. 2007) (preventing misuse of and damage to university computer network is a lawful purpose). And, based upon the information available to us, and as discussed in the prior opinion of this Office, we believe that the operation of the EINSTEIN 2.0 program falls under that exception and is reasonable under the totality of the circumstances. See *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (reasonableness of a
search under the Fourth Amendment is measured in light of the “totality of the circumstances,” balancing “on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests”) (internal quotation marks omitted; *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985) (“what is reasonable depends on the context within which a search takes place”); *O’Connor*, 480 U.S. at 726 (plurality) (reasonable workplace search must be “justified at its inception” and “reasonably related in scope to the circumstances which justified the interference in the first place”) (internal quotation marks omitted). In light of that conclusion, we also think that a federal employee’s agreement to the terms of the model log-on banner or the model computer-user agreement, or those of a banner of user agreement that are substantially equivalent to those models, constitutes valid, voluntary consent to the reasonable scope of EINSTEIN 2.0 operations. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (consent is “one of the specifically established exceptions to the requirements of both a warrant and probable cause”); *United States v. Sihler*, 562 F.2d 349 (5th Cir. 1977) (prison employee’s consent to routine search of his lunch bag valid); *cf. McDonell v. Hunter*, 807 F.2d 1302, 1310 (8th Cir. 1987) (“If a search is unreasonable, a government employer cannot require that its employees consent to that search as a condition of employment.”).

With respect to statutory issues, we have also concluded that, for the reasons set forth in our prior opinion—and so long as participating federal agencies consistently adopt, implement, and enforce model computer log-on banners or model computer-user agreements—the deployment of the EINSTEIN 2.0 program on federal information systems complies with the Wiretap Act, the Foreign Intelligence Surveillance Act, the Stored Communications Act, and the pen register and trap and trace provisions of title 18 of the United States Code. We agree with the analysis of these issues set forth in our prior opinion, and will not repeat it here.

Opinions of the Office of Legal Counsel in Volume 33

("evidence obtained from a consensual wiretap conforming to 18 U.S.C. § 2511(2)(c) is admissible in federal court proceedings without regard to state law").

/s/

DAVID J. BARRON
Acting Assistant Attorney General
KEYNOTE ADDRESS

The Developing Legal Framework for Defensive and Offensive Cyber Operations

Steven G. Bradbury*

I. Introduction

Thank you for the introduction and for inviting me to the Law School to speak at your symposium. I'm honored to be here.

The Harvard National Security Journal is outstanding, and this symposium is an excellent forum for exploring issues critical to our security and our civil liberties. I certainly found the panels today to be interesting and valuable and I learned a lot.

Unlike the participants on your panels, I'm not a noted expert on cybersecurity. But I did have the privilege to serve as head of the Office of Legal Counsel in the Department of Justice for almost five years during the last administration, and in that position I did have occasion to advise on cybersecurity issues. And I've watched developments in the area of cybersecurity since my tenure in government.

As you may know, getting to serve in the Office of Legal Counsel is something of a dream job for law nerds and for anyone who cares deeply about the Constitution and public law generally. OLC is the office that exercises the Attorney General's authority to render legal opinions to the President and the heads of the executive departments and agencies on all the most important and sensitive legal issues facing the Executive Branch. (And, believe me, that's not just interrogation!)

* Partner, Dechert, LLP. This speech was delivered as the Keynote Address at the Harvard National Security Journal Symposium, Cybersecurity: Law, Privacy, and Warfare in a Digital World (Mar 4, 2011).

Copyright © 2011 by the President and Fellows of Harvard College and Steven G. Bradbury.
When I came into OLC in 2004, I had the pleasure of serving under Jack Goldsmith, who is now, of course, an esteemed member of the faculty here at the Law School. You're also very lucky to have Jack as a member of the Advisory Board to the National Security Journal.

What I'd like to do today is to sketch out the basic legal framework that I see developing to govern the cyber operations of the federal government. I want to talk, first, about the legal framework for defensive cybersecurity activities. Then I'll address legal authorities potentially applicable to offensive cyber operations, including cyberwarfare. Lastly, I'll say a word about possible responses to WikiLeaks.

I'm speaking only for myself today — not for my law firm and not for any current or former client.

II. Defensive Cyber Security Activities

So, let's start by discussing the government's defensive cyber security activities.

Last year, in his confirmation hearing to lead the new U.S. Cyber Command, Gen. Keith Alexander, who is also Director of the National Security Agency, testified that the Defense Department's computer systems in the U.S. are bombarded with "hundreds of thousands" of hostile incursions each and every day. And that's just the Defense Department's networks.

All the computer systems of the federal government are vulnerable to infiltration and disruption from hostile foreign governments or other foreign powers, international criminal enterprises, and lone hackers.

And the concerns about network protection don't end at the outer bounds of the dot.mil or even the dot.gov cyber domains. We're also concerned about the serious national security threat to non-federal computer systems, including the networks of defense contractors working on sensitive projects, as well as the computers that control America's critical infrastructure, such as power plants and pipelines, electric grids, dams, water supply systems, air traffic control and rail transportation systems, banking systems and financial exchanges, and health care networks.
Some folks — notably, for example, Richard Clarke — have gone further and have also urged that it’s vital to our national security for the federal government to mandate steps to protect the public backbone networks of the Internet, including the major public peering points where backbone traffic is exchanged. I’m not convinced of that; I think that raises difficult issues, as I’ll touch on in a bit.

Let’s look initially at the federal government’s computer systems, and then we can work our way out from there.

**Defensive protections.** So what is the capability we want to have in place to protect our vital networks?

Certainly, we’ll want to be able to scrub the software and data inside our computer systems to find and eliminate any hostile viruses, worms, trapdoors, Trojan horses, logic bombs, etc., and to trace them back, if we can, to try to find out how they got in and where they originated.

But I want to focus now on the *perimeter* of the network, on the gateways where it connects to the public Internet or to any external web of networks beyond our control.

We’ll want to be able to detect unwanted intrusions — in real time, if possible, as they stream across the gateway. Ideally, we’d like to be able to block them before they cross the perimeter and enter the critical systems.

To spot the potentially malicious intrusions, we’ll look for the known “signatures” of previously identified malware and hostile actors. We can collect our list of malicious “signatures” from all kinds of places — from private firms that develop anti-virus software, from law enforcement units that investigate cyber crimes, from intrusions we’ve already detected in our networks, from our own intelligence agencies, and from foreign governments and their intelligence services.

The detection system will need to “learn” from new intrusions, so the list of screening signatures is constantly being refreshed.

To make this work, we’ll need sophisticated, high-speed sensors that can search the enormous volume of data traffic without an unacceptable delay in communications.
It won’t be enough to search just the “to” and “from” addressing information in each data packet; we’ll absolutely need to search down deeper, into the content of messages, since malicious code can hide in any part of a message or its attachments.

We’ll need to search outbound traffic as well as inbound, to detect the unauthorized exfiltration of sensitive information, and to identify any moles on the inside working with the infiltrators.

When we do detect a hostile intrusion, it won’t be enough just to block it. We’ll want law enforcement experts or intelligence analysts to be able to review it and we may want to take follow-up action, as necessary, directed against the source of the intrusion. That could mean action by the FBI, since maliciously disrupting or hacking into government computers is a federal crime, or it could mean action by our intelligence agencies or by the military, depending on the nature of the intrusion.

**EINSTEIN.** It turns out the Department of Homeland Security is right now rolling out an intrusion-detection system that’s designed to implement many of the capabilities I’ve just described. It’s called “EINSTEIN,” and it’s meant to protect the unclassified civilian computer networks of the federal government.

EINSTEIN will work by making a mirror copy of all the data packets passing through the gateways, and then automatically screening the duplicate data stream for any malicious signature codes.

Only the messages found to contain malicious codes will be collected and further analyzed by humans; the rest of the copied data will be immediately deleted.

And the messages that are subject to further review will be handled in accordance with established “minimization procedures,” which are requirements designed to avoid the unnecessary retention and distribution of non-public information about U.S. persons. For example, minimization would mean that the names of identified U.S. persons or content discussing U.S. persons will be masked when the message is sent on to law enforcement or intelligence agencies to the extent that such information is unnecessary to understanding the law enforcement or intelligence significance of the message.
These minimization procedures have been approved by the Attorney General, as well as by the Article III judges who sit on the Foreign Intelligence Surveillance Court.

DHS will also apply auditing and training procedures and adopt restrictions to ensure that the list of target signatures will focus only on malicious computer code and will not be used improperly to intrude on any legitimate privacy rights of the users of the network.

**Legality.** The federal government’s implementation of a system like this raises a host of legal issues involving the constitutional and statutorily protected privacy rights of Americans. So how do we approach the question of legality?

Well, we have a roadmap in the opinions the Justice Department has issued analyzing the legality of EINSTEIN.

I signed a lengthy opinion on this topic for OLC in January 2009 that memorialized DOJ’s analysis up to that point. The Obama administration adopted this opinion and made it public in August 2009, along with some follow-up advice from OLC.¹ (So, you see, it’s not true that the current administration only publishes opinions of mine when it disagrees with them!)

**Fourth Amendment protections.** The most fundamental legal restriction at issue is the Fourth Amendment, which protects against an unreasonable search by the government that infringes a person’s legitimate expectation of privacy. If the person doesn’t have a reasonable expectation of privacy in the communications reviewed, there is no “search” under the Fourth Amendment. And where there is a search, the Fourth Amendment’s basic requirement is reasonableness.

The courts have made it clear that for purposes of the Fourth Amendment, people who make a call or send an e-mail message or visit a Web site do not have a reasonable expectation of privacy in the phone

---

number called or in the addressing and routing information for an Internet communication.²

Just like an address on the outside of an ordinary envelope, the to/from addressing information or Internet routing protocol for an e-mail or Web visit is information the sender is voluntarily making available to the communications provider in order to complete the connection, and the sender can't claim a reasonable expectation that that routing information is private.

That means there would be no "search" within the meaning of the Fourth Amendment if the government screened just the "to" and "from" lines of e-mails and other IP addressing data of Internet traffic for malicious signatures.

But here, as I said, we need to go beyond that; we do need to search the content and the attachments of all Internet messages. And that would definitely implicate the privacy interests that the Fourth Amendment is concerned with.

Statutory protections. Moreover, there are a number of federal statutes that impose separate and independent privacy protections beyond the Fourth Amendment. These include:

(1) the wiretap provisions of title 18, as amended by the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq., which protect e-mail messages while in transmission;

(2) the Stored Communications Act, 18 U.S.C. § 2701 et seq., which protects electronic communications while stored in a database;

(3) the Foreign Intelligence Surveillance Act, or FISA, 50 U.S.C. § 1801 et seq., which requires special court orders for electronic surveillance of wire communications in the U.S.; and

(4) the pen register and trap and trace provisions of title 18, 18 U.S.C. § 3121 et seq., which provide protection for calling numbers and the to-and-from addressing information for e-mails.

Warrant vs. no warrant. Ordinarily, the Fourth Amendment requires that government officials obtain a warrant supported by probable cause to conduct a search. But a warrant, or any individualized court order, like a traditional FISA order or a pen register/trap and trace approval, is not possible here. We need to screen all the traffic coursing in and out of the gateway and we need to do so 24/7.

Fourth Amendment jurisprudence allows the government to conduct reasonable searches without a warrant in certain circumstances where the government has “special needs” going beyond law enforcement.

The need to protect the integrity of vital government computer networks from attack in the face of a massive number of unauthorized intrusions should constitute such a “special need,” and the various conditions, limitations, and minimization efforts that DHS will use with EINSTEIN should be sufficient to assure the reasonableness of the search.

“Rights or property.” Certain of the statutory protections at issue also permit the operator of a communications network to intercept and screen traffic on the network where and as necessary to protect the “rights or property” of the network operator.

Those provisions should also enable the government, as the network operator here, to conduct the kind of screening that EINSTEIN would entail, since it’s reasonable to believe the screening is necessary to detect and prevent harmful intrusions that could compromise the integrity of the networks.

Log-on banners and user agreements. But the federal government, with the advice of Justice Department lawyers, has settled on a simpler and broader solution as the principal legal foundation for EINSTEIN.

Each federal agency that participates in EINSTEIN will enter into a Memorandum of Agreement with DHS, and that MOA will obligate the agency to put in place detailed log-on banners, user agreements, and computer training programs for each employee, contractor, or agent who is authorized to use the agency’s computer system.
The log-on banner and user agreements will declare that the computer system is for authorized government use only, and they'll clearly state that by using the system, the employee understands and consents that he or she has no reasonable expectation of privacy in communications passing through or stored on the system; that the government may monitor, intercept, or search any data transiting or stored on the system; and that any communication or data on the system may be disclosed or used for any authorized government purpose. To access the system, the user will have to sign a consent form or click a button acknowledging and agreeing to these terms. (The Justice Department has actually used a log-on banner like this for some years now.)

All agencies whose network traffic is screened by EINSTEIN must ensure that they consistently adopt, implement, and enforce these consent and notification procedures in their computer training and usage practices.

**Fourth Amendment analysis.** DOJ concluded that the consistent application of these log-on banners and agreements will be effective in establishing as a legal matter that the users of the agency's computer network will not have a reasonable expectation of privacy in any communications they send or receive over the network.

That will go for personal communications sent over the network, too, including employees' use of the network to access their own personal Gmail or Yahoo accounts or Facebook pages.

Without a reasonable expectation of privacy, there will be no "search" within the meaning of the Fourth Amendment.

The same conclusion will apply to a private individual outside the government who communicates with the agency or with an employee of the agency, including where the individual is communicating with the employee's personal e-mail account and doesn't know that the person on the other end is accessing the account from a government network.

The Supreme Court has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and that "when a person communicates to a third party even on the understanding that the communication is confidential, he cannot object

---

if the third party conveys that information or records thereof to law enforcement authorities."

**Statutory analysis.** The log-on banners and user agreements described above will also ensure that the screening system will comply with all statutory privacy restrictions.

Each of the relevant statutes I mentioned — the Electronic Communications Privacy Act, the Stored Communications Act, FISA, and the pen register/trap and trace laws — permits the interception and disclosure of otherwise private communications if done with the "consent" of a party to the communication. Here, that means the consent of the individual employee or other user of the agency’s computers.

Thus, the wiretap provisions of title 18, as amended by ECPA, provide that “[i]t shall not be unlawful . . . for a person acting under color of law to intercept [or divulge] a[n] . . . electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception [or divulging].”

Similarly, the Stored Communications Act states that the provider of an electronic communications service “may divulge the contents of a

---

4 SEC v. Jerry T. O’Brien, Inc., 467 U.S. 735, 743 (1984). Even if it were correctly decided, the Sixth Circuit’s recent decision in United States v. Warshak holding that a person retains a reasonable expectation of privacy in personal e-mails stored with his ISP does not contradict this reasoning. See United States v. Warshak, 631 F.3d 266, 282–88 (6th Cir. 2010). While a person may reasonably expect to maintain personal control over the dissemination of e-mails he has stored on his own Web account or with his ISP, a person can no longer expect to retain control over a message he dispatches to its intended recipient. The difference is well illustrated by analogy to the world of paper files: If I send you a letter, I relinquish control over that letter to you; you’re free to share it with whomever you will, regardless of any commitment I may have gotten from you. On the other hand, if I keep a copy of the letter stored in my own filing cabinet, I retain control over dissemination of the copy and I continue to have an expectation that the copy will remain private. That expectation does not necessarily change if my filing cabinet is located in a rented storage garage, even though the proprietor of the storage garage retains a master key for necessary access to the garage. In that analogy, the proprietor of the storage garage is like the ISP in Warshak.

communication . . . with the lawful consent of the originator or an addressee or intended recipient of such communication."^{6}

And the government does not engage in "electronic surveillance" within the meaning of FISA where it intercepts the contents of a wire communication with "the consent of any party" to the communication or in circumstances where a party to the communication lacks a reasonable expectation of privacy.\(^7\)

Finally, the pen register and trap and trace provisions of title 18 do not apply to the use of such devices by the provider of an electronic communications service "where the consent of the user of th[e] service has been obtained."\(^8\) In the case of EINSTEIN, the provider of the service would be the federal government.

So that's the analysis for federal government networks.

**Expansion to certain non-federal networks.** Now, can a system like EINSTEIN be expanded to cover private or state-operated networks that contain especially sensitive information or that control the nation's most critical infrastructure? Can we apply a similar legal analysis?

It should be pretty straightforward to do so, provided the network is owned or operated by a single entity or group of entities and is set up like an intranet with a limited set of authorized users, and provided the operator can agree by contract or can be required by regulation to use log-on banners and user agreements like those employed by the federal agencies participating in EINSTEIN.

Take, for example, a defense contractor working on a classified or sensitive weapons system. The government, as a condition of the contract, could require the contractor to ensure that all sensitive information about the project is confined to a discrete network and that all persons using the network understand and agree that their communications over the network, including personal communications, will be subject to monitoring and disclosure, including disclosure to the government. The contractor would be the provider of the electronic communications service and, with the consent

---

\(^{6}\) *Id.* § 2702(b)(3).


\(^{8}\) 18 U.S.C. § 3121(b)(3).
of the users of the network, would be authorized under the various statutory provisions discussed above to conduct the monitoring of all communications on the network and make the disclosures of any communications containing malicious code. In undertaking the screening, the private party could contract with the federal government to participate in the EINSTEIN system.

I think DHS could negotiate similar cooperative arrangements with state entities and could impose similar conditions on computer networks, including private networks that are used to control the infrastructure most vital to national security. This should fall within DHS's regulatory authority over the security of "critical infrastructure."

If the non-federal network in question happens to be located in a state that requires the consent of both parties before a communication can lawfully be monitored, a valid federal requirement should preempt the state law, though in some circumstances, for example involving only contractual conditions, preemption may require an act of Congress.

**Public Internet.** What about trying to expand our intrusion-detection system out to the public Internet itself, to scour the vast streams of data that flow through the public peering points and across the gateways of the major backbone networks? Some have argued that that's the only way to achieve sufficient protection for vital U.S. computer networks.

But this is where I think I would draw the line. I don't see an easy way to dispel the legitimate privacy interests of the millions of users of the public Internet. We can't insist that they all consent to having their communications monitored, and I don't think the public would support such a policy.

Even if Congress in theory could enact some kind of sweeping legislation to impose such a regime — for example, by requiring that all ISPs be licensed and making EINSTEIN-like user agreements a condition of licensing — that's not realistic. The Internet culture would rise up in revolt, and Congress won't want to suppress the freedom and vibrancy of the Internet and risk squelching the golden goose of e-commerce.

So, one man's opinion, but I think we should focus on achieving cybersecurity for contained networks that have a discrete set of authorized
users and readily controlled gateways to the Internet. But if we can do just that much, that will go a long way toward improving our national security.

III. Offensive Cyber Operations

Okay, that’s enough about cyber security and privacy. Now let’s do a 180 and talk about the legal authorities available to the U.S. government for offensive cyber operations.

By offensive cyber operations, I’m referring to a range of potential activities that could be aimed at foreign computer systems: from straight intelligence collection (the extraction or copying of data for intelligence purposes), to counterintelligence operations (meant to deter or disrupt espionage by others against us), to covert actions conducted abroad (traditionally managed by the CIA), to cyber warfare (executed by DoD’s Cyber Command, either in support of conventional, kinetic war fighting or on a stand-alone basis).

These various kinds of operations can be authorized under different authorities using different procedures.

I should step back here and note something important: If the computer system in question is located in the United States or if it’s owned and controlled by a U.S. company or individual, it’s likely the FBI would take the lead, and the operation may be conducted as a law enforcement matter.

**Executive Order 12333.** Executive Order 12333 provides a useful launching pad for reviewing these authorities and procedures. It mirrors several provisions of the National Security Act, found in chapter 15 of title 50 of the U.S. Code.

Intelligence and counterintelligence authorities flow from the President through the Director of National Intelligence, and they’re usually vetted through an inter-agency process overseen by the National Security Council.

If they’re sufficiently sensitive, they’ll be reviewed by the principals committee of the NSC, which is typically chaired by the National Security Adviser and includes the Vice President, the Secretary of State, the
Secretary of Defense, the DNI, the Attorney General, the Chairman of the Joint Chiefs, and often the Director of the CIA. Depending on the issues involved, the principals can include the Secretary of Homeland Security and the Secretary of the Treasury. The Chief of Staff and the Counsel to the President also usually attend principals meetings.

**Covert action.** Now, what about covert action?

As defined in Executive Order 12333 and the National Security Act, “covert action,” as distinct from clandestine intelligence collection, means an operation undertaken by the U.S. government primarily designed “to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly.”

What would be an example of covert action? Well, obviously, I can’t talk about any real covert action of which I’m aware. But let’s imagine a wild, fantastical, counterfactual, and purely hypothetical scenario that bears no relation to reality: Suppose the democracy protests in the Middle East were actually organized and fomented by the United States. If that were true, the United States would not want its role to be apparent, because that would doom the effort — the local population would likely turn against the protests if they knew the United States was behind them.

Now, importantly, the definition of covert action does not include, among other things, “traditional counterintelligence activities” and “traditional military activities.” (It also excludes diplomacy, law enforcement, and pure intelligence collection, but I’m going to focus mostly on the military exception, and I’ll come back a little later to the counterintelligence exception.)

Covert action operations are traditionally conducted by the CIA with assistance as needed from the military and other intelligence agencies. Under Executive Order 12333, the National Security Council must consider each proposed covert action and present a policy recommendation to the President, along with any dissenting views.

---

9 50 U.S.C. § 413b(e).
Section 503 of the National Security Act, 50 U.S.C. § 413b, requires the President, in authorizing a covert action, to make written findings that the operation is necessary to promote identifiable foreign policy objectives and is important to the national security of the United States, and it prohibits the President from authorizing any covert action that would violate the Constitution or any statute of the United States.

Covert actions also can’t take place in the United States and can’t be used to influence U.S. policies or public opinion. (So it would be illegal if the CIA were involved in organizing the union protests in Wisconsin.)

**Congressional reporting.** The National Security Act also requires the President and DNI to ensure that the Intelligence Committees of the House and Senate are fully and currently informed of all intelligence and counterintelligence activities, to the extent consistent with the protection of sensitive sources and methods or other exceptionally sensitive matters.¹⁰

With respect to covert actions, the Act requires the President to report presidential findings supporting covert actions to the Intelligence Committees, but where the President determines that it’s essential because of “extraordinary circumstances affecting vital interests of the United States,” the President may limit access to the so-called “Gang of Eight” — the chairs and ranking members of the two Intelligence Committees, the Speaker and minority leader of the House, and the majority and minority leaders of the Senate, along with whatever other congressional leaders the President chooses to include.¹¹

The committee chairs hate when briefings are limited to the Gang of Eight, because they catch hell from the members of their committees who are outside the circle. So when former-Senator Obama first became President, there was hope among some in Congress that he would eliminate the Gang of Eight briefings. But when Congress proposed an Intelligence Authorization bill that would do just that, President Obama threatened to veto it. Once he became head of the Executive Branch, he clearly understood the importance of being able to limit the scope of briefings for the most sensitive matters. So the statute still allows for Gang of Eight briefings.

¹¹ *Id.* § 413b.
In contrast to these title 50 intelligence activities, military operations conducted under title 10 authorities are subject to oversight by the Armed Services Committees of Congress. (Title 10 of the U.S. Code governs DoD’s military authorities and the military command structure; title 50 governs the Intelligence Community and intelligence activities.)

And make no mistake, in the world of Washington, it really does matter whether an activity is characterized as covert action or a traditional military action because different Executive Branch departments or agencies will have ownership of the operation and different committees of Congress will have oversight jurisdiction, and they all jealously guard their respective domains.

**Traditional military activities.** So what is meant by “traditional military activities” and how do we apply it in classifying offensive cyber operations?

Note that it’s not the case that an operation must be treated as covert action just because the role of the United States is intended to be secret. That’s true of lots of military and counterintelligence missions as well. Think of special ops, military deception operations, or clandestine operations to prepare the environment for potential future military action.

And another thing: “traditional” can’t refer to the technology being used. The military is always at the cutting edge in developing new war fighting technologies, and information systems and computer network operations are integral parts of war in the 21st century.

One possibility is to define “traditional military activities” by reference to the laws and customs of war.

The laws of war impose a number of very important limitations on when and how military force is to be used.

These include, for example, the basic principles of non-aggression and self-defense enshrined in the United Nations Charter; the humanitarian protections and restrictions on warfare embodied in the War Crimes Act, the Geneva Conventions, and related treaties and principles of customary international law; and the laws and treaty provisions prohibiting the use of certain types of weapons, such as chemical and biological weapons.
Some of the fundamental rules of war include the principle of military necessity (that an appropriate target is one that will confer a definite military advantage), the requirement to distinguish military forces from civilian populations, the prohibition on targeting civilians and civilian objects, the principle of proportionality of response, the imperative to minimize collateral damage, the ban on perfidy, and the principle of neutrality.

One thing that distinguishes the United States from lots of other nations is the care we take to honor our international commitments. In carrying out military missions, for example, DoD is scrupulous about always trying to comply with the laws and customs of war. You may be surprised to learn that it’s quite often the norm these days for combatant commanders to make significant targeting decisions on the battlefield with the real-time input of JAG lawyers.

Military operations occur within the title 10 chain of command, which means that they’re conducted pursuant to “execute orders” from the President through the SecDef down to the combatant commanders. Execute orders usually define the general scope and purpose of the operation, and the details are filled in with operational plans and specific rules of engagement. It’s fair to assume that by the time the President signs an execute order for a particular military operation, DoD has satisfied itself that the operation can be conducted in accordance with the laws of war.

So, in my view, a good, practical way to think about “traditional military activities,” for purposes of distinguishing them from covert action, is that they can include any operation the President chooses to order the military to carry out under title 10 authorities, provided it’s consistent with the accepted norms of war.

This approach preserves critical flexibility for the President in deciding when and how to employ the military might of the United States to meet a national security threat that justifies our use of force.

It should be recognized that in the context of our armed conflict with the Taliban and international terrorist organizations like al Qaeda, there will be a range of missions, including in the realm of cyber operations, where the President can decide to use either the military option or the
covert action option, or both. They are two instruments of national policy available to the President, and they need not be mutually exclusive.

The fact that the administration is standing up a unified Cyber Command and putting such focus and resources into it suggests that the President has largely decided to conduct offensive cyber operations through the military option.

**Evolving customary law.** This approach also accommodates the reality that how the U.S. chooses to use its armed forces will significantly influence the development of customary international law.

As the label implies, customary law can evolve depending on the accepted conduct of major nations like the United States. The real-world practice of the United States in adapting the use of its military to the new challenges raised by computer warfare will (and should) help clarify the accepted customs of war in areas where the limits are not clearly established today.

And if you just review the literature on cyber war, you quickly see that that's where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects.

For example, there aren't always bright lines to tell us when a cyber attack on computer systems constitutes an "armed attack" or a "use of force" that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter.

Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. It's clearly not prohibited by the laws and customs of war.

On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law.
If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply.

But there will be gray areas in the middle. Thus, it’s far less clear that a computer assault that’s limited to deleting or corrupting data or temporarily disabling or disrupting a computer network or some specific equipment associated with the network in a way that’s not life threatening or widely destructive should be considered a use of force justifying military retaliation, even if the network belongs to the military or another government agency.

This was the case with the “distributed denial of service” attacks experienced by Estonia in 2007, which severely disrupted the country’s banking and communications systems. Suspecting that Russia was behind it, Estonia suggested that NATO declare that Estonia’s sovereignty had been attacked, which would have triggered the collective self-defense article of the NATO Treaty, but that suggestion was rebuffed on the ground that a cyber attack is not a clear military action.¹²

There’s an echo of that reasoning in Article 41 of the U.N. Charter, which says that a “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications” is not a “measure . . . involving armed force.”

And what about Stuxnet? As I understand it from public reports, Stuxnet was a computer worm that found its way into the systems controlling Iran’s nuclear program and gave faulty commands causing the destruction of the centrifuges used for enriching uranium. Suppose President Ahmadinejad claimed that Israel was behind the Stuxnet worm and claimed that Stuxnet constituted an armed attack on Iran that justified a military response against Israel. I suspect the United States would disagree.

At the same time, when it comes to a cyber attack directed against U.S. computer systems, I certainly want the President to have leeway in determining whether or not to treat the attack as a use of force that supports

military retaliation. Making such judgments is a traditional power exercised by the President, and I think he retains that leeway.

Similarly, I submit, it’s not clearly established that a cyber attack aimed at disrupting a server or Web site located in a neutral country or in a country outside a theater of open hostilities would be a violation of that country’s neutrality.

The server might be a valid military target because it’s being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations). The server might have no connection to the host country’s military, government, or critical infrastructure, and it might be readily targeted for a computer attack without inflicting widespread damage on unrelated systems used for civilian purposes.

Such a focused cyber operation — with little physical impact beyond the destruction of data or the crippling of a server — is very different from the kind of physical violation of territory — such as a conventional troop incursion or a kinetic bombing raid — that we ordinarily think of as constituting an affront to neutrality.¹³

Although every server has a physical location, the Internet is not segmented along national borders, and the enemy may gain greater tactical advantage from a server hosted halfway around the world than from one located right in the middle of hostilities.

The targeting of a server in a third country may well raise significant diplomatic difficulties (and I wouldn’t minimize those), but I don’t think the law-of-war principle of neutrality categorically precludes the President from authorizing such an operation by an executive order to Cyber Command.

**Conclusion.** So here’s my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and

¹³ A 1974 Resolution of the U.N. General Assembly, for example, defines “aggression” to mean “the use of armed force” by a state against “the sovereignty, territorial integrity or political independence” of another state. G.A. Res. 3314 (XXIX), U.N. GAOR, 29th Sess., Supp. No. 31, U.N. Doc A/9361 (Dec. 14, 1974). The focused cyber operation I’ve described hardly seems to satisfy that definition.
how the lines should be drawn on the limits of traditional military power in
the sphere of cyberspace. For example, that means that within certain
parameters, the President could decide when and to what extent military
cyber operations may target computers located outside areas of hot fighting
that the enemy is using for military advantage. And when a cyber attack is
directed at us, the President can decide, as a matter of rational policy,
whether and when to treat it as an act of war.

The corollary to all this is that in situations where the customs of war,
innovation, are not crystallized, the lawyers at the State Department and the
Justice Department shouldn’t make up new red lines — out of some
aspirational sense of what they think international law ought to be — that
end up putting dangerous limitations on the options available to the United
States. Certainly, the advice of lawyers is always important, especially so
where the legal lines are established or firmly suggested. No one would
contend that the laws of war have no application to cyber operations or that
cyberspace is a law-free zone. But it’s not the role of the lawyers to make up
new lines that don’t yet exist in a way that preempts the development of
policy. 14

In the face of this lack of clarity on key questions, some advocate for
the negotiation of a new international convention on cyberwarfare —
perhaps a kind of arms control agreement for cyber weapons. I believe there
is no foreseeable prospect that that will happen. Instead, the outlines of

14 The “Martens Clause,” found in the Hague Conventions and in Additional Protocol I to
the Geneva Conventions, does not undercut this thesis. The version of the Martens Clause
codified in Protocol I declares that on law-of-war matters not expressly addressed by treaty,
“civilians and combatants remain under the protection and authority of the principles of
international law derived from established custom, from the principles of humanity and
from the dictates of public conscience.” Protocol Additional to the Geneva Conventions of
12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts
(Protocol I) Art. 1.2, June 8, 1977, 1125 U.N.T.S. 3. There is no accepted or definitive
interpretation of this clause, see Rupert Ticehurst, The Martens Clause and the Laws of Armed
Conflict, 37 INT’L REV. RED CROSS 125 (1997); but I believe the most it can stand for is the
proposition that if there are gaps in the provisions of a treaty addressing the laws of war,
those gaps may be filled in by customary international law — i.e., the customs of war — as
established by the consistent practice of major states (and perhaps by the universal
humanitarian dictates of conscience). When there is, however, no such established and
consistent practice of states (or universal dictates of conscience) as to a particular question,
there is not a firm rule to fill in the gaps. That’s fully consistent with the notion that the
United States has flexibility as a policy matter to develop the appropriate standards it will
recognize as applicable to offensive cyber operations with respect to those key questions
about which there is no clear international norm.
accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that’s the way we should want it to work.

One final admonition I’ll offer on the topic of offensive cyber operations: In cases where the President shapes new policy by choosing military action over covert action for a cyber operation, or vice versa, I would strongly urge that the President fully brief both sets of committees in Congress — the Intelligence Committees and the Armed Services Committees — and explain the basis for the choice. It’s inevitable the committees will find out anyway when a jurisdictional marker is crossed, and it will help smooth the development of consistent policies and standards for the committee members and staff to understand and appreciate the choices made on both sides of the question.

IV. WikiLeaks

Now, as a last word, let me say something about WikiLeaks.

There’s been a lot of focus on whether to bring criminal charges against Julian Assange for the purposeful exploitation and release of classified U.S. information, including military and diplomatic communications. A criminal investigation is evidently ongoing, and I think there are strong arguments supporting that course.

But there’s also been a suggestion that we consider using offensive cyber capabilities to block or disrupt the servers overseas where WikiLeaks is holding the sensitive U.S. information.

If such an action were to be entertained, I don’t think it would be characterized as a traditional military operation (we’re not engaged in an armed conflict with WikiLeaks), and it wouldn’t have to be done as covert action. Rather, I think it could be characterized as “traditional counterintelligence activities,” which you’ll recall is another category that’s distinguished from covert action.

Executive Order 12333 defines “counterintelligence” to include, among other things, “activities conducted to ... disrupt or protect against espionage ... [or] sabotage” directed against the United States by “foreign
powers, organizations, or persons.” I think it can be argued quite easily that the WikiLeaks crusade to exfiltrate sensitive U.S. information and selectively disclose it in order to undermine and weaken American foreign policy does constitute espionage or sabotage.

But that doesn’t mean that such an operation would or should be approved. It would undoubtedly be considered an exceptionally sensitive proposal and would be thoroughly debated by the principals of the National Security Council, as contemplated by Executive Order 12333. (And I wouldn’t be surprised to learn that the principals committee actually has discussed just this possibility.)

The idea would certainly raise serious difficulties. If the servers were located in a friendly western country like Sweden, the notion of launching a cyber operation would cause major diplomatic heartburn, and the State Department would almost certainly insist that it be closely coordinated with the host country. There’s also the strong chance that any such operation would be futile. I understand from news reports that Assange has stored copies of the stolen data set on scores of servers around the world, many of which are not connected to the Internet, as well as on lots of thumb drives that he and his compatriots carry around in their backpacks.

In the end, therefore, I think the President and his advisers would probably determine that it wasn’t prudent and it wasn’t practical to rely on a cyber response to WikiLeaks. And I suspect that’s the conclusion they reached.

*   *   *

So with that anti-climax, let me end there.

Again, I really want to thank the Journal for hosting this valuable symposium, and for generously inviting me to speak. And thanks to all of you for sitting patiently through this rambling tour of cyberspace.
The Hackback Debate
BY STEPTOE ON NOVEMBER 2, 2012
POSTED IN CYBERSECURITY AND CYBERWAR, PRIVACY REGULATION, SECURITY PROGRAMS & POLICIES

The vulnerability of computer networks to hacking grows more troubling every year. No network is safe, and hacking has evolved from an obscure hobby to a major national security concern. Cybercrime has cost consumers and banks billions of dollars. Yet few cyberspies or cybercriminals have been caught and punished. Law enforcement is overwhelmed both by the number of attacks and by the technical unfamiliarity of the crimes.

Can the victims of hacking take more action to protect themselves? Can they hack back and mete out their own justice? The Computer Fraud and Abuse Act (CFAA) has traditionally been seen as making most forms of counterhacking unlawful. But some lawyers have recently questioned this view. Some of the most interesting exchanges on the legality of hacking back have occurred as dueling posts on the Volokh Conspiracy. In the interest of making the exchanges conveniently available, they are collected here a single document.

The debaters are:

• **Stewart Baker**, a former official at the National Security Agency and the Department of Homeland Security, a partner at Steptoe & Johnson with a large cybersecurity practice. Stewart Baker makes the policy case for counterhacking and challenges the traditional view of what remedies are authorized by the language of the CFAA.

• **Orin Kerr**, Fred C. Stevenson Research Professor of Law at George Washington School of Law, a former computer crimes prosecutor, and one of the most respected computer crime scholars. Orin Kerr defends the traditional view of the Act against both Stewart Baker and Eugene Volokh.

• **Eugene Volokh**, Gary T. Schwartz Professor of Law at UCLA School of Law, founder of the Volokh Conspiracy, and a sophisticated technology lawyer, presents a challenge grounded in common law understandings of trespass and tort.
Baker-Kerr

RATs and Poison: The Policy Side of Counterhacking

Stewart Baker

Good news for network security: the tools attackers use to control compromised computers are full of security holes. Undergrad students interning for Matasano Security have reverse-engineered the Remote Access Tools (RATs) that attackers use to gain control of compromised machines.

RATs, which can conduct keylogging, screen and camera capture, file management, code execution, and password-sniffing, essentially give the attacker a hook in the infected machine as well as the targeted organization.

This is great news for cybersecurity. It opens new opportunities for attribution of computer attacks, along lines I’ve suggested before: “The same human flaws that expose our networks to attack will compromise our attackers’ anonymity.”

In this case, the possibility of a true counterhack is opened up. The flaws identified by Hertz and Denbow could allow defenders to decrypt stolen documents and even to break into the attacker’s command and control link – while the attacker is still on line.

It’s only a matter of time before counterhacks become possible. The real question is whether they’ll ever become legal. Both the reporter and the security researcher agree that “legally, organizations obviously can’t hack back at the attacker.”

I believe they are wrong on the law, but first let’s explore the policy question.

Should victims be able to poison attackers’ RATs and then use the compromised RAT against their attacker?
It’s obvious to me that somebody should be able to do this. And, indeed, it seems nearly certain that somebody in the US government — using some combination of law enforcement, intelligence, counterintelligence, and covert action authorities — can do this. (I note in passing, though, that there may be no one below the President who has all these authorities, so that as a practical matter RAT poisoning may not happen without years of delay and a convulsive turf fight. That’s embarrassing, but beside the point, at least today.)

There are drawbacks to having the government do the job. It is likely that counterhacking will work best if the attacker is actually on line, when the defenders can stake out the victim’s system, give the attacker bad files, monitor the command and control machine, and to copy, corrupt, or modify ex-filtrated material. Defenders may have to swing into action with little warning.

Who will do this? Put aside the turf fight; does NSA, the FBI, or the CIA have enough technically savvy counterhackers to stake out the networks of the Fortune 500, waiting for the bad guys to show up?

Even if they do, who wants them there? Privacy campaigners will not approve of the idea of giving the government that kind of access to private networks, even networks that are under attack. For that matter, businesses with sensitive data won’t much like the stark choice of either letting foreign governments steal it all or giving the US government wide access to their networks.

On a policy perspective, surely everyone would be happier if businesses could hire their own network defenders to do battle with attackers. This would greatly reinforce the thin ranks of government investigators. It would make wide-ranging government access to private networks less necessary. And busting the government monopoly on active defense would probably increase the diversity, imagination, and effectiveness of the counterhacking community.

But there is always the pesky question of vigilantism...
First, as I’ve mentioned previously, allowing private counterhacking does not mean reverting to a Hobbesian war of all against all. Government sets rules and disciplines violators, just as it does with other privatized forms of law enforcement, from the securities industry’s FINRA to private investigators.

Second, the “vigilism” claim depends heavily on sleight of hand. Those against the idea call it “hacking back,” with the heavy implication that the defenders will blindly fire malware at whoever touches their network, laying indiscriminate waste to large swaths of the Internet. For the record, I’m against that kind of hacking back too. But RAT poison makes possible a kind of counterhacking that is far more tailored and prudent. Indeed, with such a tool, trashing the attacker’s system is dumb; it is far more valuable as an intelligence tool than for any other purpose.

Of course, the defenders will be collecting information, even if they aren’t trashing machines. And gathering information from someone else’s computer certainly raises moral and legal questions. So let’s look at the computers that RAT poisoning might allow investigators to access.

First, and most exciting, this research could allow us to short-circuit some of the cutouts that attackers use to protect themselves. Admittedly, this is beyond my technical capabilities, but it seems highly unlikely to me that an attacker can use a RAT effectively without a real-time connection from his machine to the compromised network. Sure, the attacker can run his commands through onion routers and cutout controllers. But at the end of all the hops, the attacker is still typing here and causing changes there. If the software he’s using can be compromised, then it may also be possible to inject arbitrary code into his machine and thus compromise both ends of the attacker’s communications. That’s the Holy Grail of attribution, of course.

Is there a policy problem with allowing private investigators to compromise the attacker’s machine for the purpose of gathering attribution information? Give me a break. Surely not even today’s ACLU could muster more than a flicker of concern for a thief’s right to keep his victim from recovering stolen data.
The harder question comes when the attacker is using a cutout — an intermediate command and control computer that actually belongs to someone else. In theory, gathering information on the intermediate computer intrudes on the privacy of the true owner. But, assuming that he's not a party to the crime, he has already lost control of his computer and his privacy, since the attacker is already using it freely. What additional harm does the owner suffer if the victim gathers information on his already-compromised machine about the person who attacked them both? Indeed, an intermediate command and control machine is likely to hold evidence about hundreds of other compromised networks. Most of those victims don't know they've been compromised, but their records are easy to recover from the intermediate machine once it has been accessed. Surely the social value of identifying and alerting all those victims outweighs the already attenuated privacy interest of the true owner.

In short, there's a strong policy case for letting victims of cybercrime use tools like this to counterhack their attackers. If the law forbids it, then to paraphrase Mr. Bumble, "the law is a ass, a idiot," and Congress should change it.

But I don't think the law really does prohibit counterhacking of this kind, for reasons I'll offer in a later post.

RATs and Poison Part II: The Legal Case for Counterhacking

Stewart Baker

In an earlier post, I made the policy case for counterhacking, and specifically for exploiting security weaknesses in the Remote Access Tools, or RATs, that hackers use to exploit computer networks.

There are three good reasons to poison an attacker's RAT:

- We can make sure the RAT doesn't work or that it actually tells us what the attackers are doing on our networks;
- We gain access to the command and control machines that serve
as waystations that let attackers download stolen data or upload new malware; and

- If we’re very lucky and very good, we can use the poisoned RAT to compromise the attacker’s home machine, directly identifying him and his organization.

More problematic is the legal case for counterhacking, due to long-standing opposition from the Justice Department’s Computer Crime and Intellectual Property Section, or CCIPS. Here’s what CCIPS says in its Justice Department manual on computer crime:

Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as “hacking back” into the attacker’s computer—even if such measures could in theory be characterized as “defensive.” Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, “hacking back” can damage the system of another innocent party.

This is a mix of law and policy. I’ve already explained why the Justice Department’s policy objections.

That leaves the law. Does the CFAA, prohibit counterhacking? The use of the words “may be illegal,” and “should not” are a clue that the law is at best ambiguous.

To oversimplify a bit, violations of the CFAA depend on “authorization.” If you have authorization, it’s nearly impossible to violate the CFAA, no matter what you do to a computer. If you don’t, it’s nearly impossible to avoid violating the CFAA.

But the CFAA doesn’t define “authorization.” It’s clear enough that things I do on my own computer or network are authorized. That means that the first step in poisoning a RAT is lawful. You are “authorized” under the CFAA to modify any code on your network, even if it was installed by a hacker. (For purposes of this discussion we’ll put aside copyright issues; it’s unlikely in any event that a hacker could enforce intellectual property
rights against his victim.)

The more difficult question is whether you’re “authorized” to hack into the attacker’s machine to extract information about him and to trace your files. As far as I know, that question has never been litigated, and Congress’s silence on the meaning of “authorization” allows both sides to make very different arguments. The attacker might say, “I have title to this computer; no one else has a right to look at its contents. Therefore you accessed it without authorization.” And the victim could say, “Are you kidding? It may be your computer but it’s my data, and I have a right to follow and retrieve stolen data wherever the thief takes it. Your computer is both a criminal tool and evidence of your crime, so any authorization conveyed by your title must take a back seat to mine.”

In a civil suit, the lack of definition would make both of those arguments plausible. Maybe “authorization” under the CFAA is determined solely by title; and maybe it incorporates all the constraints that law and policy put on property rights in other contexts. Personally, I dislike statutory interpretations that fly in the face of good policy, so I think the counterhacker wins that argument.

No matter; computer hackers won’t be bringing many lawsuits against their victims. The real question is whether victims can be criminally prosecuted for breaking into their attacker’s machine.

And here the answer is surely not.

The ambiguity of the statute makes a successful prosecution nearly impossible; deeply ambiguous criminal laws like this are construed in favor of the defendant. See, e.g., McBoyle v. United States, 283 U.S. 25, 27 (1931) (“[I]t is reasonable that a fair warning should be given to the world, in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible, the line should be clear.”) (Holmes, J.).

The same analysis applies even to the hardest case, where victims use a compromised RAT to access command and control machines that turn
out to be owned by an innocent third party. An innocent third party is a more appealing witness, but his machine was already compromised by hackers before the counterhacking victim came along, and it was being used as an instrumentality of crime, sufficient in some states to justify its forfeiture. It remains true that the counterhacker is pursuing his own property.

Finally, when he begins his counterhack, the victim does not know whether the intermediate machine is controlled by an attacker or by an innocent third party. Why should the law presume that it is owned by an innocent party — or force the victim to make that presumption, on pain of criminal liability? (There’s room for empirical research here; while a few years ago hackers seemed to favor compromising third-party machines for command and control, the Luckycat study suggests that some attackers now prefer to use machines and domains that they control. As the latter approach grows more common, a presumption that intermediate machines are owned by innocent third parties will grow even more artificial.)

All told, it seems reasonable to let victims counterhack a command and control machine that is exfiltrating information from the victim’s network, at least enough to determine who is in control of the machine, to identify other victims being harmed by the machine, and to follow the attacker back to his origin (or at least his next hop) if the intermediate machine is simply another victim. Requiring the victim not to counterhack if there’s uncertainty about the innocence of the machine’s owner simply gives an immunity to attackers.

The balance of equities thus seem to me to favor a recognition of the victim’s authorization to conduct at least limited surveillance of a machine that is, after all, directly involved in a violation of the victim’s rights. If “authorization” under the CFAA really boils down to a balancing of moral and social rights, and nothing in the law refutes that view, then the counterhacker has at least enough moral and social right on his side to make a criminal prosecution problematic — unless he damages the third party’s machine, in which case all bets are off.
The Legal Case Against Hack-Back: A Response to Stewart Baker

Orin Kerr

Stewart says his analysis is “surely” right. I think it’s obviously wrong. Here’s why.

The CFAA is a computer trespass statute. It prohibits accessing another person’s computer “without authorization” just like trespass laws prohibit walking on to someone else’s land without their consent. Like a traditional trespass statute, it is the owner/operator of the property that controls authorization. There is lots of disagreement about how computer owner/operators can create rights on their machines that the law will enforce but everyone agrees that hacking into someone else’s machine is the quintessential example of the kind of conduct prohibited by the statute.

Contrary to Stewart’s claim, there is no genuine ambiguity over whether the statute protects the rights of computer owners or data owners. The statutory language expressly prohibits “intentionally access[ing] a computer without authorization” (emphasis added). It protects access to computers, not access to stolen data. The rule here is the same rule that is used in real property law: The owner/operator of the property controls who has access to it. The fact that your neighbor borrowed your baseball glove and you want it back doesn’t give you a right to break into everything your neighbor owns on the theory that you can authorize yourself to go anywhere to get your glove back. The same goes for computers.

If we assume Stewart’s I-like-it-and-therefore-it-is-the-law argument were valid, I think the results it would produce would be terrible. For every one hypothetical you can devise in which such hacking back might seem like a good thing, you can come up with hundreds of examples in which it wouldn’t be. For example, wouldn’t Stewart’s theory allow copyright holders to hack into the computers of anyone suspected of having any infringing materials on their computers? That would be bad. More broadly, Stewart’s theory appears to have few limits. His test
seems to boil down to good faith: As long as someone believes that they were a victim of a computer intrusion and has a good-faith belief that they can help figure out who did this or minimize the loss of the intrusion by hacking back, the hacking back is authorized. Given the well-known difficulty of locating the source of intrusions, that’s not a power that we want to give to every person in the US who happens to own or control a computer.

Another problem with Stewart’s theory is that it would have the bizarre effect of allowing hacking victims to declare that the people who hacked into their machines can’t access their own computers. That is, if A hacks into B’s machine, B just has to announce that A now can’t use A’s own machine. If A uses his own computer, that is “without authorization” from B and therefore a crime. It’s a bizarre result, and even more bizarre given that Stewart uses the rule of lenity to justify it.

Baker Replies to Kerr

Stewart Baker

Orin Kerr and I agree that “authorization” is the central, and undefined, key to criminal liability under the CFAA. In Orin’s view, “authorization” can be determined by asking two questions: First, does the CFAA protect computers or data? And, second, who controls a computer, the data owner or the computer owner?

I believe the right answer to each question is “both.” The CFAA can and should protect both computers and data stored on computers. Similarly, more than one person can have rights to data on a computer. Orin believes that the CFAA forces a choice. If it protects computers it can’t protect data. You either have full authorization or you have none.

If anything the statute refutes that argument. The only textual clue to what the statute means by “authorized” is found in a section that imposes liability on users who exceed their authorized access to a computer; that term is defined as follows: “[T]he term ‘exceeds authorized access’ means to access a computer with authorization and
to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” Put another way, you exceed authorized access if you obtain or alter information you’re not entitled to obtain or alter.

This definition undercuts both of Orin’s assumptions about authority. And it treats “authorized” and “entitled” as more or less synonymous, which isn’t exactly consistent with the idea that authorization is all-or-nothing. If I’m attending a demonstration on the Mall, and the Park Police tell me to move on, I’m likely to say, “Sorry, but I’m entitled to be here.” As I am. But that doesn’t mean that I can then tell them to move on. They’re entitled to be there too. And what if I try to enforce my edict by taking a swing at one of them? He might say, “You’re entitled to be here, but you’re not entitled to do that here.” Quite right, too; it’s jail for me. It turns out my entitlement was real, but it was neither exclusive nor unlimited.

So too with computers under the CFAA. I may be entitled to retrieve my stolen data stolen from a machine without being entitled to take the machine to a pawn shop and sell it, or to tell the innocent owner what he can and cannot do with it.

And what about policy? Which reading of the statute produces better results?

To understand the policy consequences of the choice, let’s begin with a reminder of our strategic situation. Right now, every computer and network in the country is vulnerable to intrusion by authoritarian foreign governments if not criminals.

The intruders have one clear vulnerability; they collect this stolen data on command-and-control machines, which may in some cases belong to other innocent victims. Victims could gain access to these machines, could render the stolen information worthless, could gather clues about the attackers, and could even identify hundreds of other victims who probably don’t yet know they’ve been compromised. That would be a very good thing.
In Orin’s world, though, it’s illegal. Under his reading of the law, the hundreds of victims go unnotified, the evidence goes ungathered, the stolen data goes, well, to China, until law enforcement gets around to the cyber equivalent of stolen-bicycle paperwork.

And what of all those bad policy outcomes that Orin conjures – the crazed vigilantes and the RIAA rummaging in everyone’s computers? The answer is that we, or at least the courts, don’t have to recognize their authority to do that. The courts don’t have to treat “good faith” as creating a counterhacking entitlement; they could as easily insist on a higher standard, such as probable cause. They could recognize the counterhacker’s authority to gather evidence but not to harm innocent third parties, just as they distinguish today between demonstrators who are entitled to throw insults but not punches on park property. They could reject the notion that the copying of 99-cent music files justifies the same response as a campaign to compromise every network in the country. They could distinguish, in short, between baby and bathwater.

It’s true that my definition of authorization is more complicated than Orin’s, that it requires more line-drawing. But so does life. Orin’s alternative is as simple — and as unjust — as applying the murder laws equally to serial killers and to homeowners who shoot home invaders. Nothing in law or policy requires that we adopt such a reading.

**More on Hacking Back: Kerr Replies to Baker**

**Orin Kerr**

Stewart makes a textual argument and a policy argument. I find both extremely weak.

Stewart’s first argument is that it’s possible to read the statute as giving authorization rights to people who have rights in data rather than rights in computers because the statute doesn’t textually distinguish between computers and underlying data.

If you read the whole statute, though, that’s plainly wrong. The statute repeatedly and consistently distinguishes between computers and data.
The elements of the statute dealing with rights with computers are covered by the basic unauthorized access concept common to most of the different crimes listed in 18 U.S.C. 1030(a). In contrast, the elements dealing with data are covered by the additional elements Congress required for the additional offenses listed in 1030(a). It’s one of the most basic divisions in the statute.

As I read the statute Congress was pretty careful to distinguish rights to computers — the trespass into the machine, covered by the unauthorized access prohibition — from rights to data — the extra elements of 1030(a) for the different crimes that Congress created. Given that, I don’t think it makes textual sense to read the unauthorized access prohibition as governed by rights in data. The statute is just not as mystifying and unclear as Stewart claims. (Also, what does it mean to “own” data? If someone copies this blog post and saves it on their computer without my consent, can I hack into the computer because I “own” that data? Concepts such as “owning” data and when data becomes “stolen” are notoriously difficult to work with — indeed, 18 U.S.C. 1030 was passed so that such questions didn’t need to be asked. It seems puzzling to reintroduce them sub silentio here.)

Second, is Stewart’s policy argument: Justice demands this reading of the statute because the Chinese are invading our computers and we need to stop them. In his post, Stewart suggests that a proper jurisprudential sophistication frees judges to do whatever they want with the statute to deal with the Chinese. With their newfound sense of sophistication, judges should go forth and devise a set of principles for interpreting “authorization” by which it is not a crime for big US companies to go after their stolen data when the Chinese take that data while it is still illegal for people to hack back when they’re not very good at it, the RIAA wants to do it, or there isn’t really a good reason for it. Stewart doesn’t actually offer any legal basis for that distinction. He doesn’t have an argument for where the line should be or even what principles should be used to interpret authorization. He just wants judges to go figure this stuff out somehow.

If someone needs to figure this stuff out, though, it’s a job for Congress
instead of the courts. Stewart isn’t just reading the statute. He’s asking judges to write a new statute that he thinks would be better than the one we now have. Maybe Congress should consider the kind of exception Stewart wants. It’s hard to tell, as Stewart hasn’t told us what the new statute should look like. (Instead, he has only told us the result the statute should reach on one case.) But as long as we’re only talking about what the statute presently means — that is, what Congress passed already, and what courts have to interpret — I don’t see a plausible way to read “authorization” to get to the result Stewart wants.

If I were Stewart, I would try to rely on the necessity defense instead of creative readings of authorization to get where he wants to go. Stewart’s argument is best made not as the claim that this isn’t unauthorized, but that it is unauthorized conduct justified by the specific circumstances he has in mind. That’s an argument for the affirmative defense of necessity. Necessity is a nice and vague exception, which is helpful for Stewart’s purposes. It’s a controversial exception as a matter of federal law, but at least there’s some support for it. And it seems to be really what Stewart has in mind. In my view, it would be better to try to make that argument directly rather than by appeals to justice or interpretations of “authorization.”

Baker’s Last Response

Stewart Baker

Now the debate with Orin is actually getting somewhere. Sort of. Here’s a scorecard:

1. Does authorization depend exclusively on ownership?

Orin’s latest post does a good job of showing that the CFAA often draws a coherent distinction between rights in data and rights in a computer, and that rights in the computer are the statute’s principal focus. I don’t disagree.

Where we differ is how much that matters. Orin seems convinced that this distinction makes rights in data irrelevant to the question of what
constitutes authorized access to a computer. He doesn’t really offer a reason for treating it as irrelevant. He just assumes it must be, probably because he also assumes that authorization is an all or nothing concept, so that if the owner has authorization no one else has any, and vice versa.

But Orin’s assumption has no basis in the statute that I can see. As my last response says, that’s like assuming that because a trespass statute protects the owners of land, everyone else must be punished as a trespasser, no matter what other rights they have to enter the property. That would make felons of rescuers, people in hot pursuit of thieves, easement holders, and government officials. You could come to that conclusion if that’s what the law unequivocally said, but in this case the law only makes felons of people who are not authorized (or not entitled) to access the computer.

So why would we ignore other claims of entitlement – especially when ignoring those claims makes a felon of someone performing an act with undeniable social value?

Orin’s reluctance to defend his assumption is striking. Maybe he’s got a good response; but he hasn’t offered it yet.

2. Should policy influence the interpretation of “authorization”? 

Orin continues to look down his nose at the introduction of policy into the interpretation of this central but undefined term. He thinks I’m requesting a new statute. In fact I’m asking the courts to recognize a perfectly plausible reading of “authorization,” in a criminal context where ambiguity would ordinarily be resolved in favor of the defendant.

I agree with Orin that this interpretation requires the courts to decide which entitlements should be recognized and which should not. He thinks that’s a role for Congress, not the courts, an argument that might be more persuasive in discussing a civil statute, or a criminal statute that was not deterring companies from responding aggressively to a dangerous intelligence attack on our economy and our society.
That said, I welcome Orin’s acknowledgement that maybe Congress should permit counterhacking in some circumstances. Though I fear the CCIPS Old Guard lives on in his heart, and that somehow no actual amendment will ever quite pass muster there.

3. Is necessity a defense for counterhacking?

Orin suggests that a federal criminal necessity defense might be more apt in this case. Maybe so, but he acknowledges that it is at best controversial. At worst, in fact, it doesn’t exist. So, while I won’t spurn even a modest agreement with Orin, the chance to prove an affirmative defense that may not apply isn’t likely to offer much comfort for companies that want to gather information about their attackers.

A Final Response on Hacking Back

Orin Kerr

Thanks to Stewart for the interesting exchange on the (un)lawfulness of hacking back. Here are my concluding thoughts.

First, Stewart repeatedly draws analogies to the law of physical trespass that are faulty because they misunderstand the law of physical trespass. Stewart seems to think that it is legal to break into someone else’s house to retrieve your property stored inside. He also assumes that it is always okay for “rescuers, people in hot pursuit of thieves, easement holders, and government officials” to enter private property. From these assumptions, Stewart guesses that trespass law doesn’t apply to such cases because the conduct is authorized and thus can’t be a trespass. He builds his proposal on that assumption. Just treat electronic trespass like physical trespass, he says: Hack back is authorized just like analogous physical entries are authorized.

But trespass law doesn’t work that way. First, you don’t have a right to break into someone else’s house to retrieve your stuff. That’s a trespass. The issue comes up most often in criminal cases when a party who entered someone else’s home and took property is charged with trespass and burglary. It’s common for the defense to claim that that
they entered to retrieve their own property: They thus concede liability for a criminal trespass but deny liability for the more serious crime of burglary. Cf. Auman v. People, 109 P.3d 647 (Colo. 2005). Similarly, those who are rescuers or police officers or those in hot pursuit don't have a general exemption from trespass liability. Instead, they have to invoke an affirmative defense. Rescuers must invoke the necessity defense. See, e.g., City of Wichita v. Tilson, 253 Kan. 285 (1993). Police officers must invoke the affirmative defense of the Fourth Amendment. Either they have to produce a valid warrant or they have to identify an applicable exception to the warrant clause (one of which is hot pursuit). See, e.g., Entick v. Carrington, 95 Eng. Rep. 807 (K.B. 1765); Warden v. Hayden, 387 U.S. 294 (1967). Easement holders can’t trespass, but that's because easements limit the property owner’s usual right to exclude.

What’s the lesson from physical trespass laws? It’s that trespass liability is actually pretty broad, and the kinds of exceptions that Stewart is using for purposes of analogy are a lot more limited than Stewart thinks. They’re affirmative defenses, not elements of the crime itself. So while I agree that we should treat physical trespass and cybertrespass the same way that means recognizing that hacking back violates 18 U.S.C. 1030 and that the only way to get out of liability is to fit the case into an affirmative defense.

What about the affirmative defense of necessity? It seems to respond to Stewart’s concerns. If any existing criminal law doctrine fits Stewart’s argument, that’s it. Stewart says it isn’t very helpful, though, because it “isn’t likely to offer much comfort for companies that want to gather information about their attackers.” It’s too doctrinally uncertain and vague for companies to rely on safely. I'll concede that’s true. But how is it relevant? We’re just debating what the law is. What companies feel about that law is irrelevant to the question.

A final comment

Stewart Baker
I still don’t think we’ve quite engaged. My point in discussing the various trespass exceptions is not to import them into the CFAA. My point is that trespass does not turn entirely on title, because the law recognizes that there are times when a right to enter the property is allowed. That’s significant not for the precise content of the right but because the CFAA uses language ("authorization," "entitlement") that directly invites an examination of the rights of the intruder.

You might say that "authorization" doesn’t exactly invite a claim of moral right by the person accused of a CFAA violation. But the statute does equate authorization with entitlement, which does invite such a claim. And the Budapest Convention, which is a more or less direct translation of the CFAA into treaty-speak, goes even further, criminalizing access "without right." Surely this invites defendants to say, "I didn’t access that computer without right. I have a right to pursue my data."

Put another way, by using such an open-ended word as "authorization," you could say that the CFAA incorporated the defense of necessity into the crime, along with other claims of right or entitlement. The Justice Department might say that incorporating such a vague and ambiguous defense into the statute is unfair because it makes prosecutions harder. But it was the Justice Department that chose the term in the first place, precisely because it is so ambiguous and capacious that it allowed prosecution of wrongdoers without much worry about changes in technology. To which I would reply, "That’s fine, CCIPS, but you have to take the good with the bad. If ‘authority’ stretches with the times for you, then it stretches with the times for the defendant."

In fact, let’s carry that point just a bit further for illustrative purposes. CCIPS could have written a (slightly) more capacious and ambiguous statute making it a felony to "do wrong with a computer." Under that even more future-proofed law it would surely be open to a defendant to argue that counterhacking is not wrong. It seems to me that "authorization" is a slightly more precise and certainly fancier-sounding variant of "doing wrong."

I still don’t know why Orin thinks that this reading of "authorization" is
plainly wrong.

***

Volokh-Kerr

The Rhetoric of Opposition to Self-Help:

Eugene Volokh

I was just talking to some people recently about the question of "digital self-defense" — whether organizations that are under cyberattack should be free to (and are free to) fight back against attacking sites by trying to bring those sites down, by hacking into the sites, and so on.

I don’t claim to know the definitive answer to this question; but I did want to say a few words about some common anti-self-help rhetorical tropes, which are sometimes heard both in this context and other contexts.

1. Vigilantism: Allowing digital self-defense (or, to be precise, digital defense of property), the argument goes, would mean sanctioning vigilantism; the nonvigilante right solution is to leave matters to law enforcement.

Yet the law has never treated defense of property as improper "vigilantism." American law bars you from punishing those who attack you or your property, but it has always allowed you to use force to stop the attack, or prevent an imminent attack. There are limits on the use of force, such as the principle that generally (though not always) property may be defended only with nonlethal force. But generally speaking the use of force is allowed, and shouldn’t be tainted with the pejorative term of “vigilantism,” which connotes illegality. (Black’s Law Dictionary echoes this, defining vigilantism as “The act of a citizen who takes the law into his or her own hands by apprehending and punishing suspected criminals.”)

2. Taking the Law Into Your Own Hands: Critics of self-defense and defense of property also sometimes characterize it as “taking the law
into your own hands.” This too implies, it seems to me, extralegal action, through which someone unlawfully taking into his own hands power that the law leaves only in law enforcement’s hands.

Yet the law has always placed in your own hands — or, if you prefer, has never taken away from your own hands — the right to defend yourself and your property (subject to certain limits). By using this right, you aren’t taking the law into your own hands. You’re using the law that has always been in your hands.

There are many reasons the law has allowed such self-defense and defense of property: It’s generally more immediate than what law enforcement can do; even after the fact, law enforcement is often stretched too thin even to investigate all crimes; sometimes law enforcement may be biased against certain people, and may not take their requests for help seriously, so self-help is the only game in town. There are also reasons to limit self-defense and defense of property (I’ll note a few below). But let’s not assume that self-defense and defense of property somehow involve unlawful arrogation of legal authority on the defenders’ part. Rather, they generally involve legally authorized exercise of legal authority.

3. **But the Statute Has No Self-Defense Exceptions:** Ah, some may say, perhaps in the physical world you have the right to defend yourself and your property — but the CFAA secures no such right, so whatever one’s views on self-help, the fact is that self-help is illegal.

Yet, surprising as it may seem to many, self-defense and defense of property may be allowed even without express statutory authorization. These defenses were generally recognized by judges, back when the criminal law was generally judge-made; and many jurisdictions don’t expressly codify them even now. Federal law, for instance, has no express “self-defense” or “defense of property” statute. The federal statute governing assaults within federal maritime and territorial jurisdiction simply says, in part,

   Whoever, within the special maritime and territorial jurisdiction of the
United States, is guilty of an assault shall be punished as follows ....

(4) Assault by striking, beating, or wounding, by a fine under this title or imprisonment for not more than six months, or both.

(5) Simple assault, by a fine under this title or imprisonment for not more than six months, or both, or if the victim of the assault is an individual who has not attained the age of 16 years, by fine under this title or imprisonment for not more than 1 year, or both.

(6) Assault resulting in serious bodily injury, by a fine under this title or imprisonment for not more than ten years, or both.

(7) Assault resulting in substantial bodily injury to an individual who has not attained the age of 16 years, by fine under this title or imprisonment for not more than 5 years, or both.

Assault is generally defined (more or less) as “any intentional attempt or threat to inflict injury upon someone else, when coupled with an apparent present ability to do so, and includes any intentional display of force that would give a reasonable person cause to expect immediate bodily harm, whether or not the threat or attempt is actually carried out or the victim is injured.” The federal criminal code thus on its face prohibits all assaults, including ones done to defend one’s life. Yet self-defense is a perfectly sound defense under federal law — because federal courts recognize self-defense as a general criminal defense, available even when the statute doesn’t specifically mention it.

Likewise, federal law generally bans possession of firearms by felons, with no mention of self-defense as a defense. Yet federal courts have recognized an exception for felons’ picking up a gun in self-defense against an imminent deadly threat, again because self-defense is a common-law defense available in federal prosecutions generally.

Given this, a federal statute’s general prohibition on breaking into another’s computer doesn’t dispose of breakins done in defense of property against imminent threat — just as federal statutes’ general prohibitions on assault or on possession of a firearm by a felon don’t
dispose of assault or possession done in defense of life (or sometimes property) against imminent threat. Federal criminal law already includes judicially recognized and generally available self-defense and defense of property defenses, even when the defendant is prosecuted under a statute that doesn’t expressly mention such defenses.

There still remains a good deal of uncertainty about how the defense of property defense would play out in any particular digital strikeback situation, and I suppose it’s possible that courts might even decide that it’s categorically unavailable as a matter of law in computer breakin cases (though it would be unusual, given the general availability of self-defense and defense of property defenses). But it is a mistake to simply assert that such a defense is unavailable simply because the statute doesn’t mention it.

***

All this having been said, I want to stress that there are plausible arguments in favor of prohibiting digital self-defense (either criminalizing it or making it tortious), and reasons to be skeptical about easy analogies between digital self-defense (or, more precisely, defense of property) and physical self-defense. It may be, for instance, that there’s more of a risk of error in digital self-defense cases, in that you might disable, directly or indirectly, a computer that’s not actually attacking you. (Say, for instance, you’re defending against a worm by launching a counterworm; there’s more risk of massive damage to many third parties from an error in the counterworm than there is in a typical situation where you’re confronting someone who’s trying to run off with your bicycle.) It’s also not obvious what should be allowed when you’re going after a computer that is attacking you but only because it’s been hijacked. Should that turn, for instance, on whether the computer’s owner was negligent in allowing the computer to be hijacked?

It’s also not clear how the general principle that defense of property must generally be nonlethal should play out — what if you’re under attack using a hijacked computer that belongs to a hospital, an airport, a 911 center, or some other life-critical application? Is disabling that computer
potentially lethal force, because it may have lethal consequences? How can you tell whether the computer is indeed running some application on which lives turn?

It's therefore not obvious whether the law should criminalize most or all forms of digital self-defense, criminalize some and make others tortious, leave it entirely to the tort system so long as the actor sincerely believed (or perhaps reasonably believed) the actions were necessary to defend his property, or whatever else. Some limits on digital defense of property may well be proper, especially if we think that on balance allowing such defense would lead to too much harm to the property of third parties. But we need to analyze things carefully, by asking some of the questions I noted in the last few paragraphs — not just by condemning digital self-defense as vigilantism, as taking the law into one's own hands, or as clearly illegal under current computer crime law.

Thanks to Warren Stramiello, a student whose paper first alerted me to the defense of property analogy; and note the Journal of Law, Economics & Policy symposium on the subject, which is available in volume 1, issue 1 of the Journal, but unfortunately not on the Web. (Participants included our very own Orin Kerr, as well as my incoming colleague Doug Lichtman.)

A Response to Eugene Volokh

Orin Kerr


First, I highly doubt that a defendant can assert a "digital self-help" claim in a prosecution brought under the CFAA, 18 U.S.C. 1030. Eugene is right that federal criminal statutes generally do not mention self-defense and other defenses, and yet courts sometimes have recognized those defenses for some crimes. But I don't think it's accurate to say, as Eugene does, that "federal criminal law already includes judicially
recognized and generally available self-defense and defense of property
defenses.” Some commentators have said this, but I believe it clashes
with the Supreme Court's most recent take on such questions in Dixon v.

As I read Dixon, it seems that whether a federal defense exists is a
question of Congressional intent. Specifically, the question is whether
and how Congress meant to incorporate the common law defenses when
it enacted that particular crime. Where Congress was silent, courts are
supposed to reconstruct what Congress probably wanted or would have
wanted “in an offense-specific context.” Id. at 2447. (It's true
that Dixon was a duress case, not a self-defense case, but it cited the
Cannabis opinion, which was a necessity case; to me that suggests that
the Court sees all the common law defenses together.)

This is pretty straightforward when considering a federal criminal law that
closely tracks a traditional criminal prohibition, such as homicide. As
Justice Kennedy put it in his concurrence in Dixon, “When issues of
congressional intent with respect to the nature, extent, and definition of
federal crimes arise, we assume Congress acted against certain
background understandings set forth in judicial decisions in the Anglo-
American legal tradition.” It’s hard to imagine Congress enacting a
homicide statute without meaning to incorporate a self-defense
provision. So in that context, courts have readily applied self-defense
even though it’s not technically written into the statute.

I think the CFAA is quite different. I don't know of any evidence that
anyone in Congress had ever even heard about “hacking back” when
Congress passed the CFAA in 1986. Congress did consider whether
there were some kind of computer intrusions that would be okay based
on the context; specifically, it created an exception in 1030(f) exempting
“any lawfully authorized investigative, protective, or intelligence activity
of a law enforcement agency.” But it didn’t create an exception for self-
defense, and I don't know of any reason to think that there was a
background sense that those defenses would apply as seems to be
required under Dixon. Given that, I would tend to doubt that a federal
“cyber self-defense” doctrine exists.
Although it's not directly contrary to Eugene's post, I'll also add my 2 cents that I think such a defense would be a really, really, really bad idea. Here's an excerpt of what I wrote on the topic in a 2005 article, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability*:

It is very easy to disguise the source of an Internet attack. Internet packets do not indicate their original source. Rather, they indicate the source of their most immediate hop. Imagine I have an account from computer A, and that I want to attack computer D. I will direct my attack from computer A to computer B, from B to computer C, and from C to computer D. The victim at computer D will have no idea that the attack is originating at A. He will see an attack coming from computer C. Further, the use of a proxy server or anonymizer can easily disguise the actual source of attack. These services route traffic for other computers, and make it appear to a downstream victim as if the attack were coming from a different source.

As a result, the chance that a victim of a cyber attack can quickly and accurately identify where the attack originates is quite small. By corollary, the chance that an initial attacker would be identified by his victim and could be attacked back successfully is also quite small. Further, if the law actually encouraged victims of computer crime to attack back at their attackers, it would create an obvious incentive for attackers to be extra careful to disguise their location or use someone else's computer to launch the attack. In this environment, rules encouraging offensive self-help will not deter online attacks. A reasonably knowledgeable cracker can be confident that he can attack all day with little chance of being hit back. The assumption that an attacker can be identified and targeted may have been true in the Wild West, but tends not to be true for an Internet attack.

Legalizing self-help would also encourage foul play designed to harness the new privileges. One possibility is the bankshot attack: If I want a computer to be attacked, I can route attacks through that one computer towards a series of victims, and then wait for the victims to attack back at that computer because they believe the computer is
the source of the attack. By harnessing the ability to disguise the origin of attack, a wrongdoer can get one innocent party to attack another. Indeed, any wrongdoer can act as a catalyst to a chain reaction of hacking back and forth among innocent parties. Imagine that I don’t like two businesses, A and B. I can launch a denial-of-service attack at the computers of A disguised to look like it originates from the computers at B. The incentives of self-help will do the rest. A will defend itself by launching a counterattack at B’s computers. B, thinking it is under attack from A, will then launch an attack back at A. A will respond back at B; B back at A; and so on. As these examples suggest, basing a self-help strategy on the virtual model of the Wild West does not reflect a realistic picture of the Internet. Self-help in cyberspace would almost certainly lead to more computer misuse, not less.

More in the article itself (unfortunately, the version on SSRN is only an early draft, but the final is on Westlaw and Lexis.)

Response to Orin Kerr

Eugene Volokh

Common-Law Federal Criminal Defenses:

I just wanted to very briefly comment on Orin’s post on the subject. Dixon v. United States involved the question of who is to bear the burden of proof as to a duress defense. The “long-established common-law rule” had been that the defendant must prove duress by a preponderance of the evidence, and the Court held that Congress did not intend to displace this rule. This is where the “offense-specific context” language comes up (citation omitted):

Congress can, if it chooses, enact a duress defense that places the burden on the Government to disprove duress beyond a reasonable doubt. In light of Congress’ silence on the issue, however, it is up to the federal courts to effectuate the affirmative defense of duress as Congress “may have contemplated” it in an offense-specific context.
In the context of the firearms offenses at issue — as will usually be the case, given the long-established common-law rule — we presume that Congress intended the petitioner to bear the burden of proving the defense of duress by a preponderance of the evidence.

It seems to me that this common-law tradition is the most important factor here, and the longstanding common-law acceptance of the defense-of-property defense should lead federal courts to assume that Congress didn’t mean to preempt it, at least absence a statement from Congress to the contrary.

It’s true that Congress likely didn’t think much about the defense when enacting computer crime laws; but the point of the common-law criminal defenses is precisely that the legislature often doesn’t think much about defenses, which often (as with duress, for instance) involve relatively rare circumstances. The defenses are out there to be used when the triggering circumstances arise, and Congress doesn’t need to think much about them when enacting specific statutes.

So it seems to me that Dixon is quite consistent with my position: Congress legislates against the background of various common-law rules related to criminal law defenses, and the general presumption is that Congress doesn’t mean to displace these background rules.

Response to Eugene Volokh

Orin Kerr

More on the “Hacking Back” Defense: I wanted to add one more round to the exchange Eugene and I were having about whether a defendant charged with a federal computer intrusion crime can assert a “hacking back” defense. I’m still of the opinion that defendants cannot assert such a defense, and I wanted to respond specifically to Eugene’s most recent post about it. Specifically, I want to make two points. First, I’m not entirely sure a general defense of property defense doctrine exists as a default in federal criminal law, and second, if the doctrine exists I don’t think it covers computer intrusions.
The reason I'm unsure that the "defense of property" defense exists as a Congressional default is that the defense seems to be quite rare in federal court, and the cases appear almost entirely in a very specific context. Based on a quick Westlaw check, at least, I could only find about 30 federal criminal cases that seem to apply it or discuss it at all. Further, those cases arise in almost entirely in a very specific context: a defense raised in a prosecution for physical assault. There's also a bit of homicide and one or other two crimes thrown in, but not much. Perhaps a lot more cases exist beyond what I could find, but I couldn't find much — and what I found was quite narrow and applied only on in a very small subset of criminal cases. Clearly this doesn't rule out that Congress legislates all criminal offense against a general background norm of a "defense of property" defense being available, but I think it does shed some doubt on it.

Second, when stated as a defense in federal criminal cases, "defense of property" seems to mean only defense of physical property from physical access or removal. For example, in the context of the Model Penal Code's defense of property section, which has been influential in federal court applications of defenses, the provisions are available only "to prevent or terminate an unlawful entry or other trespass upon land or a trespass against or the unlawful carrying away of tangible, movable property . . . , [or] to effect an entry or re-entry upon land or to retake tangible movable property." MPC 3.06. (The MPC seems to treat the kind of interference with property that includes computer intrusions under a separate section, § 3.10, Justification in Property Crimes, which seems to foillow a different set of principles. Also, while you might think "entry" includes virtual entry, entry in the context of criminal trespass statutes are generally understood to mean physical entry.) Given that, it seems that whatever "defense of property" doctrine is established as a background norm when Congress creates a new criminal law, it doesn't seem to me to apply to computer attacks.

Anyway, I should stress that we don't yet have any cases on this, so both Eugene and I are guessing as to what courts would or should do based on the legal materials out there. It's a very interesting question. Finally, I'll just add further thoughts in the comment thread in the future,
as I'm not sure a lot of readers are interested in this issue.

Response to Orin Kerr

Eugene Volokh

The "Defense of Property" Defense:

I much appreciate Orin's posts on the subject, and I should note again what I noted at the outset — there are quite plausible policy arguments for barring "hacking back" even when it's done to defend property against an ongoing attack, and Orin has expressed some of them in the past. That an action falls generally within the ambit of an existing defense, or is closely analogous to an existing defense, doesn't preclude the conclusion that we should nonetheless bar the action because of special problems associated with it.

Nonetheless, I do disagree with two parts of Orin's analysis. First, it seems to me that the defense-of-property defense has indeed been recognized as part of a general class of common-law defenses — including justifications such as self-defense and defense of others, and excuses such as duress or insanity — that are by default accepted in all jurisdictions, or at least all jurisdictions that have not expressly codified their defenses. (I say "by default"; they may be expressly statutorily precluded, as a few states have done as to insanity.) Robinson's treatise on Criminal Law Defenses describes it well, I think,

Every American jurisdiction recognizes a justification for the defense of property. The principle of the defense of property is analogous to that of all defensive force justifications and may be stated as follows: ... Conduct constituting an offense is justified if:

(1) an aggressor unjustifiably threatens the property of another; and

(2) the actor engages in conduct harmful to the aggressor

(a) when and to the extent necessary to protect the property,
(b) that is reasonable in relation to the harm threatened.

More generally, defense of property, self-defense, and defense of others are generally treated by the law more or less similarly, though subject to the general principle that defense of property will generally not justify the use of lethal force. I have never seen in any case, treatise, or other reference any indication that federal law differs from this, and rejects the notion that defense-of-property is a general default.

I agree with Orin that the defense has been rare. But I suspect that it is rare because defense of property generally doesn’t authorize the use of deadly force, and because use of supposedly defensive nondeadly force is less likely to draw a federal prosecutor’s attention than the use of supposedly defensive deadly force. The typical nonlethal defense of property scenario — someone says I punched him, and I claim I did this in order to keep him from stealing my briefcase — just isn’t likely to end up prosecuted by the local U.S. Attorney’s office, even if there’s some reason to doubt my side of the story.

Second, Orin points to the Model Penal Code as evidence that “when stated as a defense in federal criminal cases, ‘defense of property’ seems to mean only defense of physical property from physical access or removal”; and the MPC does define defense of property as limited to “use of force upon or toward the person of another ... to prevent or terminate an unlawful entry or other trespass upon land or a trespass against or the unlawful carrying away of tangible, movable property ..., [or] to effect an entry or re-entry upon land or to retake tangible movable property” (plus provides for a related but different defense in § 3.10).

But the MPC seems to define defenses in a way that’s focused on those crimes that the MPC covers. For instance, the MPC’s self-defense provision literally covers only “the use of force upon or toward another person”; it would not cover imminent self-defense as a defense to a charge of being a felon in possession of a firearm (though no such crime is defined by the MPC in the first place). Yet federal law does recognize this. Likewise, state cases recognize self-defense as a defense to the use of force against an animal, when the use would otherwise be illegal
(I could find no federal prosecutions involving the question).

Now perhaps the answer is that federal law would reject even self-defense as a defense to non-physical-force crimes, and that the defense in felon-in-possession cases is actually a species of the necessity defense. But if that’s true (which isn’t clear, since it’s not even clear that federal law recognizes a general necessity defense), then one could equally argue for digital self-defense under the rubric of necessity.

Likewise, while Orin brackets § 3.10, that might very well be the defense-of-property provision (though labeled by the MPC under the more general rubric of “justification in property crimes”) that an MPC-following federal court might adopt, if it chooses to take a narrow view of the common-law defense-of-property defense. Section 3.10 generally allows “intrusion on or interference with property [when tort law would recognize] a defense of privilege in a civil action based [on the conduct],” unless the relevant criminal statute “deals with the specific situation involved” or a “legislative purpose to exclude the justification claimed otherwise plainly appears.” And the common law has generally recognized defense of property as a privilege in civil actions. (See, e.g., Restatement (Second) of Torts § 79, which allows even nonlethal physical force against a person when necessary to terminate the person’s intrusion on your possession of chattels. That doesn’t literally cover use of nonlethal electronic actions against a computer, but the point of common-law defenses is that they are applicable by analogy; the Restatement is thus a guide, not a detailed code to be followed only according to its literal terms even in novel situations.)

So we have to remember, it seems to me, that the federal law of criminal defenses is common law, borrowing from both the substance of the traditionally recognized common-law defenses, and from the common-law method, which involves reasoning by analogy. The common-law method also allows analogies to be resisted, if the new situation is vastly different from the old; and of course Congress can trump common-law defenses by statute. But the background remains that there’s a common-law defense of defense of property (buttressed, where necessary, by the necessity defense, and to the extent one is influenced by the Model
Penal Code, by § 3.10's borrowing from the common-law tort defenses), and that there's no reason to think that federal law takes a narrow view of this defense.
PANEL VI:

ETHICAL ISSUES FACING LAWYERS PRACTICING NATIONAL SECURITY LAW

MODERATOR:
ALBERT C. HARVEY
PREAMBLE: A LAWYER'S RESPONSIBILITIES

[1] A lawyer, as a member of the legal profession, is a representative of clients, an officer of the legal system and a public citizen having special responsibility for the quality of justice.

[2] As a representative of clients, a lawyer performs various functions. As advisor, a lawyer provides a client with an informed understanding of the client's legal rights and obligations and explains their practical implications. As advocate, a lawyer zealously asserts the client's position under the rules of the adversary system. As negotiator, a lawyer seeks a result advantageous to the client but consistent with requirements of honest dealings with others. As an evaluator, a lawyer acts by examining a client's legal affairs and reporting about them to the client or to others.

[3] In addition to these representational functions, a lawyer may serve as a third-party neutral, a nonrepresentational role helping the parties to resolve a dispute or other matter. Some of these Rules apply directly to lawyers who are or have served as third-party neutrals. See, e.g., Rules 1.12 and 2.4. In addition, there are Rules that apply to lawyers who are not active in the practice of law or to practicing lawyers even when they are acting in a nonprofessional capacity. For example, a lawyer who commits fraud in the conduct of a business is subject to discipline for engaging in conduct involving dishonesty, fraud, deceit or misrepresentation. See Rule 8.4.

[4] In all professional functions a lawyer should be competent, prompt and diligent. A lawyer should maintain communication with a client concerning the representation. A lawyer should keep in confidence information relating to representation of a client except so far as disclosure is required or permitted by the Rules of Professional Conduct or other law.

[5] A lawyer's conduct should conform to the requirements of the law, both in professional service to clients and in the lawyer's business and personal affairs. A lawyer should use the law's procedures only for legitimate purposes and not to harass or intimidate others. A lawyer should demonstrate respect for the legal system and for those who serve it, including judges, other
lawyers and public officials. While it is a lawyer's duty, when necessary, to challenge the rectitude of official action, it is also a lawyer's duty to uphold legal process.

[6] As a public citizen, a lawyer should seek improvement of the law, access to the legal system, the administration of justice and the quality of service rendered by the legal profession. As a member of a learned profession, a lawyer should cultivate knowledge of the law beyond its use for clients, employ that knowledge in reform of the law and work to strengthen legal education. In addition, a lawyer should further the public's understanding of and confidence in the rule of law and the justice system because legal institutions in a constitutional democracy depend on popular participation and support to maintain their authority. A lawyer should be mindful of deficiencies in the administration of justice and of the fact that the poor, and sometimes persons who are not poor, cannot afford adequate legal assistance. Therefore, all lawyers should devote professional time and resources and use civic influence to ensure equal access to our system of justice for all those who because of economic or social barriers cannot afford or secure adequate legal counsel. A lawyer should aid the legal profession in pursuing these objectives and should help the bar regulate itself in the public interest.

[7] Many of a lawyer's professional responsibilities are prescribed in the Rules of Professional Conduct, as well as substantive and procedural law. However, a lawyer is also guided by personal conscience and the approbation of professional peers. A lawyer should strive to attain the highest level of skill, to improve the law and the legal profession and to exemplify the legal profession's ideals of public service.

[8] A lawyer's responsibilities as a representative of clients, an officer of the legal system and a public citizen are usually harmonious. Thus, when an opposing party is well represented, a lawyer can be a zealous advocate on behalf of a client and at the same time assume that justice is being done. So also, a lawyer can be sure that preserving client confidences ordinarily serves the public interest because people are more likely to seek legal advice, and thereby heed their legal obligations, when they know their communications will be private.

[9] In the nature of law practice, however, conflicting responsibilities are encountered. Virtually all difficult ethical problems arise from conflict between a lawyer's responsibilities to clients, to the legal system and to the lawyer's own interest in remaining an ethical person while earning a satisfactory living. The Rules of Professional Conduct often prescribe terms for resolving such conflicts. Within the framework of these Rules,
however, many difficult issues of professional discretion can arise. Such issues must be resolved through the exercise of sensitive professional and moral judgment guided by the basic principles underlying the Rules. These principles include the lawyer's obligation zealously to protect and pursue a client's legitimate interests, within the bounds of the law, while maintaining a professional, courteous and civil attitude toward all persons involved in the legal system.

[10] The legal profession is largely self-governing. Although other professions also have been granted powers of self-government, the legal profession is unique in this respect because of the close relationship between the profession and the processes of government and law enforcement. This connection is manifested in the fact that ultimate authority over the legal profession is vested largely in the courts.

[11] To the extent that lawyers meet the obligations of their professional calling, the occasion for government regulation is obviated. Self-regulation also helps maintain the legal profession's independence from government domination. An independent legal profession is an important force in preserving government under law, for abuse of legal authority is more readily challenged by a profession whose members are not dependent on government for the right to practice.

[12] The legal profession's relative autonomy carries with it special responsibilities of self-government. The profession has a responsibility to assure that its regulations are conceived in the public interest and not in furtherance of parochial or self-interested concerns of the bar. Every lawyer is responsible for observance of the Rules of Professional Conduct. A lawyer should also aid in securing their observance by other lawyers. Neglect of these responsibilities compromises the independence of the profession and the public interest which it serves.

[13] Lawyers play a vital role in the preservation of society. The fulfillment of this role requires an understanding by lawyers of their relationship to our legal system. The Rules of Professional Conduct, when properly applied, serve to define that relationship.

SCOPE

[14] The Rules of Professional Conduct are rules of reason. They should be interpreted with reference to the purposes of legal representation and of the law itself. Some of the Rules are imperatives, cast in the terms "shall" or "shall not." These define proper conduct for purposes of professional discipline. Others, generally cast in the term "may," are permissive and define areas under the Rules in which the lawyer has discretion to exercise professional judgment. No disciplinary action should be taken when the lawyer chooses not to act or acts within the bounds of
such discretion. Other Rules define the nature of relationships between the lawyer and others. The Rules are thus partly obligatory and disciplinary and partly constitutive and descriptive in that they define a lawyer's professional role. Many of the Comments use the term "should." Comments do not add obligations to the Rules but provide guidance for practicing in compliance with the Rules.

[15] The Rules presuppose a larger legal context shaping the lawyer's role. That context includes court rules and statutes relating to matters of licensure, laws defining specific obligations of lawyers and substantive and procedural law in general. The Comments are sometimes used to alert lawyers to their responsibilities under such other law.

[16] Compliance with the Rules, as with all law in an open society, depends primarily upon understanding and voluntary compliance, secondarily upon reinforcement by peer and public opinion and finally, when necessary, upon enforcement through disciplinary proceedings. The Rules do not, however, exhaust the moral and ethical considerations that should inform a lawyer, for no worthwhile human activity can be completely defined by legal rules. The Rules simply provide a framework for the ethical practice of law.

[17] Furthermore, for purposes of determining the lawyer's authority and responsibility, principles of substantive law external to these Rules determine whether a client-lawyer relationship exists. Most of the duties flowing from the client-lawyer relationship attach only after the client has requested the lawyer to render legal services and the lawyer has agreed to do so. But there are some duties, such as that of confidentiality under Rule 1.6, that attach when the lawyer agrees to consider whether a client-lawyer relationship shall be established. See Rule 1.18. Whether a client-lawyer relationship exists for any specific purpose can depend on the circumstances and may be a question of fact.

[18] Under various legal provisions, including constitutional, statutory and common law, the responsibilities of government lawyers may include authority concerning legal matters that ordinarily repose in the client in private client-lawyer relationships. For example, a lawyer for a government agency may have authority on behalf of the government to decide upon settlement or whether to appeal from an adverse judgment. Such authority in various respects is generally vested in the attorney general and the state's attorney in state government, and their federal counterparts, and the same may be true of other government law officers. Also, lawyers under the supervision of these officers may be authorized to represent several government
agencies in intragovernmental legal controversies in circumstances where a private lawyer could not represent multiple private clients. These Rules do not abrogate any such authority.

[19] Failure to comply with an obligation or prohibition imposed by a Rule is a basis for invoking the disciplinary process. The Rules presuppose that disciplinary assessment of a lawyer's conduct will be made on the basis of the facts and circumstances as they existed at the time of the conduct in question and in recognition of the fact that a lawyer often has to act upon uncertain or incomplete evidence of the situation. Moreover, the Rules presuppose that whether or not discipline should be imposed for a violation, and the severity of a sanction, depend on all the circumstances, such as the willfulness and seriousness of the violation, extenuating factors and whether there have been previous violations.

[20] Violation of a Rule should not itself give rise to a cause of action against a lawyer nor should it create any presumption in such a case that a legal duty has been breached. In addition, violation of a Rule does not necessarily warrant any other nondisciplinary remedy, such as disqualification of a lawyer in pending litigation. The Rules are designed to provide guidance to lawyers and to provide a structure for regulating conduct through disciplinary agencies. They are not designed to be a basis for civil liability. Furthermore, the purpose of the Rules can be subverted when they are invoked by opposing parties as procedural weapons. The fact that a Rule is a just basis for a lawyer's self-assessment, or for sanctioning a lawyer under the administration of a disciplinary authority, does not imply that an antagonist in a collateral proceeding or transaction has standing to seek enforcement of the Rule. Nevertheless, since the Rules do establish standards of conduct by lawyers, a lawyer's violation of a Rule may be evidence of breach of the applicable standard of conduct.

[21] The Comment accompanying each Rule explains and illustrates the meaning and purpose of the Rule. The Preamble and this note on Scope provide general orientation. The Comments are intended as guides to interpretation, but the text of each Rule is authoritative.
Rule 1.1: Competence

Client-Lawyer Relationship

Rule 1.1 Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
Comment on Rule 1.1

Client-Lawyer Relationship
Rule 1.1 Competence - Comment

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impractical. Even in an emergency, however, assistance should be limited to that reasonably necessary in the circumstances, for ill-considered action under emergency conditions can jeopardize the client's interest.

[4] A lawyer may accept representation where the requisite level of competence can be achieved by reasonable preparation. This applies as well to a lawyer who is appointed as counsel for an unrepresented person. See also Rule 6.2.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry
into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client regarding the scope of the representation may limit the matters for which the lawyer is responsible. See Rule 1.2(c).

Retaining or Contracting With Other Lawyers

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer’s own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and must reasonably believe that the other lawyers’ services will contribute to the competent and ethical representation of the client. See also Rules 1.2 (allocation of authority), 1.4 (communication with client), 1.5(e) (fee sharing), 1.6 (confidentiality), and 5.5(a) (unauthorized practice of law). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer’s own firm will depend upon the circumstances, including the education, experience and reputation of the nonfirm lawyers; the nature of the services assigned to the nonfirm lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

[7] When lawyers from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other and the client about the scope of their respective representations and the allocation of responsibility among them. See Rule 1.2. When making allocations of responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.
Rule 1.6: Confidentiality of Information

Client-Lawyer Relationship
Rule 1.6 Confidentiality Of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(6) to comply with other law or a court order; or

(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
Comment on Rule 1.6

Client-Lawyer Relationship
Rule 1.6 Confidentiality Of Information - Comment

[1] This Rule governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client. See Rule 1.18 for the lawyer's duties with respect to information provided to the lawyer by a prospective client, Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client and Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

[3] The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. See also Scope.
Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. A lawyer’s use of a hypothetical to discuss issues relating to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client or the situation involved.

Authorized Disclosure

Except to the extent that the client’s instructions or special circumstances limit that authority, a lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. Lawyers in a firm may, in the course of the firm’s practice, disclose to each other information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers.

Disclosure Adverse to Client

Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions. Paragraph (b) (1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial threat that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town’s water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer’s disclosure is necessary to eliminate the threat or reduce the number of victims.

Paragraph (b)(2) is a limited exception to the rule of confidentiality that permits the lawyer to reveal information to the extent necessary to enable affected persons or appropriate authorities to prevent the client from committing a crime or fraud, as defined in Rule 1.0(d), that is reasonably certain to result in substantial injury to the financial or property interests of another and in furtherance of which the client has used or is using the lawyer’s services. Such a serious abuse of the client-
lawyer relationship by the client forfeits the protection of this Rule. The client can, of course, prevent such disclosure by refraining from the wrongful conduct. Although paragraph (b)(2) does not require the lawyer to reveal the client’s misconduct, the lawyer may not counsel or assist the client in conduct the lawyer knows is criminal or fraudulent. See Rule 1.2(d). See also Rule 1.16 with respect to the lawyer’s obligation or right to withdraw from the representation of the client in such circumstances, and Rule 1.13(c), which permits the lawyer, where the client is an organization, to reveal information relating to the representation in limited circumstances.

[8] Paragraph (b)(3) addresses the situation in which the lawyer does not learn of the client’s crime or fraud until after it has been consummated. Although the client no longer has the option of preventing disclosure by refraining from the wrongful conduct, there will be situations in which the loss suffered by the affected person can be prevented, rectified or mitigated. In such situations, the lawyer may disclose information relating to the representation to the extent necessary to enable the affected persons to prevent or mitigate reasonably certain losses or to attempt to recoup their losses. Paragraph (b)(3) does not apply when a person who has committed a crime or fraud thereafter employs a lawyer for representation concerning that offense.

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer's personal responsibility to comply with these Rules. In most situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.

[10] Where a legal claim or disciplinary charge alleges complicity of the lawyer in a client's conduct or other misconduct of the lawyer involving representation of the client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. The same is true with respect to a claim involving the conduct or representation of a former client. Such a charge can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, for example, a person claiming to have been defrauded by the lawyer and client acting together. The lawyer's right to respond arises when an assertion of such complicity has been made. Paragraph (b)(5) does not require the lawyer to await the commencement of an action or proceeding that charges such complicity, so that the defense may be established by responding
directly to a third party who has made such an assertion. The right to defend also applies, of course, where a proceeding has been commenced.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Other law may require that a lawyer disclose information about a client. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of information relating to the representation appears to be required by other law, the lawyer must discuss the matter with the client to the extent required by Rule 1.4. If, however, the other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

Detection of Conflicts of Interest

[13] Paragraph (b)(7) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, such as when a lawyer is considering an association with another firm, two or more firms are considering a merger, or a lawyer is considering the purchase of a law practice. See Rule 1.17, Comment [7]. Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only once substantive discussions regarding the new relationship have occurred. Any such disclosure should ordinarily include no more than the identity of the persons and entities involved in a matter, a brief summary of the general issues involved, and information about whether the matter has terminated. Even this limited information, however, should be disclosed only to the extent reasonably necessary to detect and resolve conflicts of interest that might arise from the possible new relationship. Moreover, the disclosure of any information is prohibited if it would compromise the attorney-client privilege or otherwise prejudice the client (e.g., the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possibility of divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under those circumstances, paragraph (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer's fiduciary duty to the lawyer's firm may also govern a lawyer's conduct when exploring an association with another firm and is beyond the scope of these
Rules.

[14] Any information disclosed pursuant to paragraph (b)(7) may be used or further disclosed only to the extent necessary to detect and resolve conflicts of interest. Paragraph (b)(7) does not restrict the use of information acquired by means independent of any disclosure pursuant to paragraph (b)(7). Paragraph (b)(7) also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, see Comment [5], such as when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation.

[15] A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4. Unless review is sought, however, paragraph (b)(6) permits the lawyer to comply with the court's order.

[16] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified. Where practicable, the lawyer should first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose. If the disclosure will be made in connection with a judicial proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[17] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). In exercising the discretion conferred by this Rule, the lawyer may consider such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction and factors that may extenuate the conduct in question. A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule.
Disclosure may be required, however, by other Rules. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). See Rules 1.2(d), 4.1(b), 8.1 and 8.3. Rule 3.3, on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this Rule. See Rule 3.3(c).

**Acting Competently to Preserve Confidentiality**

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer’s duties when sharing information with nonlawyers outside the lawyer’s own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the
extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Former Client

[20] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.

Back to Rule | Table of Contents | Next Comment
Rule 1.11: Special Conflicts of Interest for Former & Current Government Officers & Employees

Client-Lawyer Relationship
Rule 1.11 Special Conflicts Of Interest For Former And Current Government Officers And Employees

(a) Except as law may otherwise expressly permit, a lawyer who has formerly served as a public officer or employee of the government:

(1) is subject to Rule 1.9(c); and

(2) shall not otherwise represent a client in connection with a matter in which the lawyer participated personally and substantially as a public officer or employee, unless the appropriate government agency gives its informed consent, confirmed in writing, to the representation.

(b) When a lawyer is disqualified from representation under paragraph (a), no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter unless:

(1) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and

(2) written notice is promptly given to the appropriate government agency to enable it to ascertain compliance with the provisions of this rule.

(c) Except as law may otherwise expressly permit, a lawyer having information that the lawyer knows is confidential government information about a person acquired when the lawyer was a public officer or employee, may not represent a private client whose interests are adverse to that person in a matter in which the information could be used to the material disadvantage of that person. As used in this Rule, the term "confidential government information" means information that has been obtained under governmental authority and which, at the time this Rule is applied, the government is prohibited by law from disclosing to the public or has a legal privilege not to disclose and which is not otherwise available to the public. A firm with which that lawyer is associated may undertake or continue representation in the matter only if the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom.

(d) Except as law may otherwise expressly permit, a lawyer
currently serving as a public officer or employee:

(1) is subject to Rules 1.7 and 1.9; and

(2) shall not:

(i) participate in a matter in which the lawyer participated personally and substantially while in private practice or nongovernmental employment, unless the appropriate government agency gives its informed consent, confirmed in writing; or

(ii) negotiate for private employment with any person who is involved as a party or as lawyer for a party in a matter in which the lawyer is participating personally and substantially, except that a lawyer serving as a law clerk to a judge, other adjudicative officer or arbitrator may negotiate for private employment as permitted by Rule 1.12(b) and subject to the conditions stated in Rule 1.12(b).

(e) As used in this Rule, the term "matter" includes:

(1) any judicial or other proceeding, application, request for a ruling or other determination, contract, claim, controversy, investigation, charge, accusation, arrest or other particular matter involving a specific party or parties, and

(2) any other matter covered by the conflict of interest rules of the appropriate government agency.
Comment on Rule 1.11

Client-Lawyer Relationship
Rule 1.11 Special Conflicts Of Interest For Former And Current Government Officers And Employees - Comment

[1] A lawyer who has served or is currently serving as a public officer or employee is personally subject to the Rules of Professional Conduct, including the prohibition against concurrent conflicts of interest stated in Rule 1.7. In addition, such a lawyer may be subject to statutes and government regulations regarding conflict of interest. Such statutes and regulations may circumscribe the extent to which the government agency may give consent under this Rule. See Rule 1.0(e) for the definition of informed consent.

[2] Paragraphs (a)(1), (a)(2) and (d)(1) restate the obligations of an individual lawyer who has served or is currently serving as an officer or employee of the government toward a former government or private client. Rule 1.10 is not applicable to the conflicts of interest addressed by this Rule. Rather, paragraph (b) sets forth a special imputation rule for former government lawyers that provides for screening and notice. Because of the special problems raised by imputation within a government agency, paragraph (d) does not impute the conflicts of a lawyer currently serving as an officer or employee of the government to other associated government officers or employees, although ordinarily it will be prudent to screen such lawyers.

[3] Paragraphs (a)(2) and (d)(2) apply regardless of whether a lawyer is adverse to a former client and are thus designed not only to protect the former client, but also to prevent a lawyer from exploiting public office for the advantage of another client. For example, a lawyer who has pursued a claim on behalf of the government may not pursue the same claim on behalf of a later private client after the lawyer has left government service, except when authorized to do so by the government agency under paragraph (a). Similarly, a lawyer who has pursued a claim on behalf of a private client may not pursue the claim on behalf of the government, except when authorized to do so by paragraph (d). As with paragraphs (a)(1) and (d)(1), Rule 1.10 is not applicable to the conflicts of interest addressed by these paragraphs.

[4] This Rule represents a balancing of interests. On the one
hand, where the successive clients are a government agency and
another client, public or private, the risk exists that power or
discretion vested in that agency might be used for the special
benefit of the other client. A lawyer should not be in a position
where benefit to the other client might affect performance of the
lawyer's professional functions on behalf of the government.
Also, unfair advantage could accrue to the other client by reason
of access to confidential government information about the
client's adversary obtainable only through the lawyer's
government service. On the other hand, the rules governing
lawyers presently or formerly employed by a government agency
should not be so restrictive as to inhibit transfer of employment
to and from the government. The government has a legitimate
need to attract qualified lawyers as well as to maintain high
ethical standards. Thus a former government lawyer is
disqualified only from particular matters in which the lawyer
participated personally and substantially. The provisions for
screening and waiver in paragraph (b) are necessary to prevent
the disqualification rule from imposing too severe a deterrent
against entering public service. The limitation of disqualification
in paragraphs (a)(2) and (d)(2) to matters involving a specific
party or parties, rather than extending disqualification to all
substantive issues on which the lawyer worked, serves a similar
function.

[5] When a lawyer has been employed by one government
agency and then moves to a second government agency, it may
be appropriate to treat that second agency as another client for
purposes of this Rule, as when a lawyer is employed by a city
and subsequently is employed by a federal agency. However,
because the conflict of interest is governed by paragraph (d), the
latter agency is not required to screen the lawyer as paragraph
(b) requires a law firm to do. The question of whether two
government agencies should be regarded as the same or different
clients for conflict of interest purposes is beyond the scope of
these Rules. See Rule 1.13 Comment [9].

[6] Paragraphs (b) and (c) contemplate a screening arrangement.
See Rule 1.0(k) (requirements for screening procedures). These
paragraphs do not prohibit a lawyer from receiving a salary or
partnership share established by prior independent agreement,
but that lawyer may not receive compensation directly relating
the lawyer's compensation to the fee in the matter in which the
lawyer is disqualified.

[7] Notice, including a description of the screened lawyer's prior
representation and of the screening procedures employed,
generally should be given as soon as practicable after the need
for screening becomes apparent.
[8] Paragraph (c) operates only when the lawyer in question has knowledge of the information, which means actual knowledge; it does not operate with respect to information that merely could be imputed to the lawyer.

[9] Paragraphs (a) and (d) do not prohibit a lawyer from jointly representing a private party and a government agency when doing so is permitted by Rule 1.7 and is not otherwise prohibited by law.

[10] For purposes of paragraph (e) of this Rule, a "matter" may continue in another form. In determining whether two particular matters are the same, the lawyer should consider the extent to which the matters involve the same basic facts, the same or related parties, and the time elapsed.
Rule 1.13: Organization as Client

Client-Lawyer Relationship
Rule 1.13 Organization As Client

(a) A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.

(b) If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action, intends to act or refuses to act in a matter related to the representation that is a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, then the lawyer shall proceed as is reasonably necessary in the best interest of the organization. Unless the lawyer reasonably believes that it is not necessary in the best interest of the organization to do so, the lawyer shall refer the matter to higher authority in the organization, including, if warranted by the circumstances to the highest authority that can act on behalf of the organization as determined by applicable law.

(c) Except as provided in paragraph (d), if

(1) despite the lawyer's efforts in accordance with paragraph (b) the highest authority that can act on behalf of the organization insists upon or fails to address in a timely and appropriate manner an action, or a refusal to act, that is clearly a violation of law, and

(2) the lawyer reasonably believes that the violation is reasonably certain to result in substantial injury to the organization,

then the lawyer may reveal information relating to the representation whether or not Rule 1.6 permits such disclosure, but only if and to the extent the lawyer reasonably believes necessary to prevent substantial injury to the organization.

(d) Paragraph (c) shall not apply with respect to information relating to a lawyer's representation of an organization to investigate an alleged violation of law, or to defend the organization or an officer, employee or other constituent associated with the organization against a claim arising out of an alleged violation of law.

(e) A lawyer who reasonably believes that he or she has been discharged because of the lawyer's actions taken pursuant to paragraphs (b) or (c), or who withdraws under circumstances
that require or permit the lawyer to take action under either of those paragraphs, shall proceed as the lawyer reasonably believes necessary to assure that the organization's highest authority is informed of the lawyer's discharge or withdrawal.

(f) In dealing with an organization's directors, officers, employees, members, shareholders or other constituents, a lawyer shall explain the identity of the client when the lawyer knows or reasonably should know that the organization's interests are adverse to those of the constituents with whom the lawyer is dealing.

(g) A lawyer representing an organization may also represent any of its directors, officers, employees, members, shareholders or other constituents, subject to the provisions of Rule 1.7. If the organization's consent to the dual representation is required by Rule 1.7, the consent shall be given by an appropriate official of the organization other than the individual who is to be represented, or by the shareholders.
Comment on Rule 1.13

Client-Lawyer Relationship
Rule 1.13 Organization As Client - Comment

The Entity as the Client

[1] An organizational client is a legal entity, but it cannot act except through its officers, directors, employees, shareholders and other constituents. Officers, directors, employees and shareholders are the constituents of the corporate organizational client. The duties defined in this Comment apply equally to unincorporated associations. "Other constituents" as used in this Comment means the positions equivalent to officers, directors, employees and shareholders held by persons acting for organizational clients that are not corporations.

[2] When one of the constituents of an organizational client communicates with the organization's lawyer in that person's organizational capacity, the communication is protected by Rule 1.6. Thus, by way of example, if an organizational client requests its lawyer to investigate allegations of wrongdoing, interviews made in the course of that investigation between the lawyer and the client's employees or other constituents are covered by Rule 1.6. This does not mean, however, that constituents of an organizational client are the clients of the lawyer. The lawyer may not disclose to such constituents information relating to the representation except for disclosures explicitly or impliedly authorized by the organizational client in order to carry out the representation or as otherwise permitted by Rule 1.6.

[3] When constituents of the organization make decisions for it, the decisions ordinarily must be accepted by the lawyer even if their utility or prudence is doubtful. Decisions concerning policy and operations, including ones entailing serious risk, are not as such in the lawyer's province. Paragraph (b) makes clear, however, that when the lawyer knows that the organization is likely to be substantially injured by action of an officer or other constituent that violates a legal obligation to the organization or is in violation of law that might be imputed to the organization, the lawyer must proceed as is reasonably necessary in the best interest of the organization. As defined in Rule 1.0(f), knowledge can be inferred from circumstances, and a lawyer cannot ignore the obvious.

[4] In determining how to proceed under paragraph (b), the lawyer should give due consideration to the seriousness of the violation and its consequences, the responsibility in the
organization and the apparent motivation of the person involved, the policies of the organization concerning such matters, and any other relevant considerations. Ordinarily, referral to a higher authority would be necessary. In some circumstances, however, it may be appropriate for the lawyer to ask the constituent to reconsider the matter; for example, if the circumstances involve a constituent's innocent misunderstanding of law and subsequent acceptance of the lawyer's advice, the lawyer may reasonably conclude that the best interest of the organization does not require that the matter be referred to higher authority. If a constituent persists in conduct contrary to the lawyer's advice, it will be necessary for the lawyer to take steps to have the matter reviewed by a higher authority in the organization. If the matter is of sufficient seriousness and importance or urgency to the organization, referral to higher authority in the organization may be necessary even if the lawyer has not communicated with the constituent. Any measures taken should, to the extent practicable, minimize the risk of revealing information relating to the representation to persons outside the organization. Even in circumstances where a lawyer is not obligated by Rule 1.13 to proceed, a lawyer may bring to the attention of an organizational client, including its highest authority, matters that the lawyer reasonably believes to be of sufficient importance to warrant doing so in the best interest of the organization.

[5] Paragraph (b) also makes clear that when it is reasonably necessary to enable the organization to address the matter in a timely and appropriate manner, the lawyer must refer the matter to higher authority, including, if warranted by the circumstances, the highest authority that can act on behalf of the organization under applicable law. The organization's highest authority to whom a matter may be referred ordinarily will be the board of directors or similar governing body. However, applicable law may prescribe that under certain conditions the highest authority reposes elsewhere, for example, in the independent directors of a corporation.

**Relation to Other Rules**

[6] The authority and responsibility provided in this Rule are concurrent with the authority and responsibility provided in other Rules. In particular, this Rule does not limit or expand the lawyer's responsibility under Rules 1.8, 1.16, 3.3 or 4.1. Paragraph (c) of this Rule supplements Rule 1.6(b) by providing an additional basis upon which the lawyer may reveal information relating to the representation, but does not modify, restrict, or limit the provisions of Rule 1.6(b)(1) - (6). Under paragraph (c) the lawyer may reveal such information only when the organization's highest authority insists upon or fails to address threatened or ongoing action that is clearly a violation of law,
and then only to the extent the lawyer reasonably believes necessary to prevent reasonably certain substantial injury to the organization. It is not necessary that the lawyer's services be used in furtherance of the violation, but it is required that the matter be related to the lawyer's representation of the organization. If the lawyer's services are being used by an organization to further a crime or fraud by the organization, Rules 1.6(b)(2) and 1.6(b)(3) may permit the lawyer to disclose confidential information. In such circumstances Rule 1.2(d) may also be applicable, in which event, withdrawal from the representation under Rule 1.16(a)(1) may be required.

[7] Paragraph (d) makes clear that the authority of a lawyer to disclose information relating to a representation in circumstances described in paragraph (c) does not apply with respect to information relating to a lawyer's engagement by an organization to investigate an alleged violation of law or to defend the organization or an officer, employee or other person associated with the organization against a claim arising out of an alleged violation of law. This is necessary in order to enable organizational clients to enjoy the full benefits of legal counsel in conducting an investigation or defending against a claim.

[8] A lawyer who reasonably believes that he or she has been discharged because of the lawyer's actions taken pursuant to paragraph (b) or (c), or who withdraws in circumstances that require or permit the lawyer to take action under either of these paragraphs, must proceed as the lawyer reasonably believes necessary to assure that the organization's highest authority is informed of the lawyer's discharge or withdrawal.

**Government Agency**

[9] The duty defined in this Rule applies to governmental organizations. Defining precisely the identity of the client and prescribing the resulting obligations of such lawyers may be more difficult in the government context and is a matter beyond the scope of these Rules. See Scope [18]. Although in some circumstances the client may be a specific agency, it may also be a branch of government, such as the executive branch, or the government as a whole. For example, if the action or failure to act involves the head of a bureau, either the department of which the bureau is a part or the relevant branch of government may be the client for purposes of this Rule. Moreover, in a matter involving the conduct of government officials, a government lawyer may have authority under applicable law to question such conduct more extensively than that of a lawyer for a private organization in similar circumstances. Thus, when the client is a governmental organization, a different balance may be appropriate between maintaining confidentiality and assuring that
the wrongful act is prevented or rectified, for public business is involved. In addition, duties of lawyers employed by the
government or lawyers in military service may be defined by
statutes and regulation. This Rule does not limit that authority.
See Scope.

Clarifying the Lawyer's Role

[10] There are times when the organization's interest may be or
become adverse to those of one or more of its constituents. In
such circumstances the lawyer should advise any constituent,
whose interest the lawyer finds adverse to that of the
organization of the conflict or potential conflict of interest, that
the lawyer cannot represent such constituent, and that such
person may wish to obtain independent representation. Care must
be taken to assure that the individual understands that, when
there is such adversity of interest, the lawyer for the organization
cannot provide legal representation for that constituent
individual, and that discussions between the lawyer for the
organization and the individual may not be privileged.

[11] Whether such a warning should be given by the lawyer for
the organization to any constituent individual may turn on the
facts of each case.

Dual Representation

[12] Paragraph (g) recognizes that a lawyer for an organization
may also represent a principal officer or major shareholder.

Derivative Actions

[13] Under generally prevailing law, the shareholders or
members of a corporation may bring suit to compel the directors
to perform their legal obligations in the supervision of the
organization. Members of unincorporated associations have
essentially the same right. Such an action may be brought
nominally by the organization, but usually is, in fact, a legal
controversy over management of the organization.

[14] The question can arise whether counsel for the organization
may defend such an action. The proposition that the organization
is the lawyer's client does not alone resolve the issue. Most
derivative actions are a normal incident of an organization's
affairs, to be defended by the organization's lawyer like any other
suit. However, if the claim involves serious charges of
wrongdoing by those in control of the organization, a conflict
may arise between the lawyer's duty to the organization and the
lawyer's relationship with the board. In those circumstances, Rule
1.7 governs who should represent the directors and the
organization.
Ethical Ethics Advice: A Department of Defense

Department of Defense Ethics Rules are often complex; their application, however, does not need to be. Whether the product of poor ethics advice or a misunderstanding and misapplication of the ethics rules, many of the transgressions mentioned within this article were, in the final analysis, likely preventable if more care, thought, and effort had been proactively applied. Further, just as DOD leaders and personnel must act ethically, DOD ethics counselors must act ethically when crafting ethics advice. Simply put, ethics counselors must provide ethical ethics advice.

BY COL. JOSEPH P. "DUTCH" BIALKE
Counselor’s 12-Minute “Light Read”

“R
c
elativity applies to physics, not
e
thics.”
—Albert Einstein

Institutional Military Ethics and Leadership

Various ethical improprieties by a number of leaders and personnel within the Department of Defense have recently included, among other abuses, the acceptance of unauthorized gifts, misuse of government vehicles, unauthorized Official Representation Fund (ORF) expenditures, false claims and travel vouchers, misuse of Temporary Duty Assignments (TDVs), unauthorized upgraded travel, improper expenditures of appropriated funds, unauthorized upgraded hotel accommodations, inappropriate use of government property and resources, misuse of subordinates, improper non-Federal Entity (NFE) endorsements/fundraising/membership drives, unauthorized spousal travel, and unauthorized military air travel.¹

In accordance with the Joint Ethics Regulation (JER), the heads of Department of Defense component commands or organizations are personally accountable in maintaining their respective commands’ ethics programs.² Given this responsibility, senior military officers and civil servants are expected to display personal leadership in the area of ethics and ethical conduct. Ethics is and must continue to be leadership-driven. Institutional ethics is first and foremost a commander’s program. Leaders are charged with the affirmative duty and responsibility of promoting a strong organizational ethical culture. To effectively support leaders in this fundamental obligation, ethics advisors must consistently provide them ethical advice.

“We must vigilantly protect and reinforce ethics as a central element of our workplace culture. Even the perception of unethical behavior or impropriety must be avoided ... I ask that you continue to ... be a visible role model of ethical behavior, hold yourself and others accountable, and ensure an ethical culture is a hallmark of the organizations you lead.”
—Memorandum from Secretary of Defense Leon Panetta to the secretaries of the military departments, chairman of the Joint Chiefs of Staff, et al, Subject: Ethics, Integrity, and Accountability, 2 May 2012

Military Readiness and the Positive Impact of Ethics Compliance

“While we are guarding the country, we must accept being the guardian of the finest ethics. The country needs it and we must do it.”

Institutional military ethics is a force-multiplier. Ethics compliance directly facilitates military efficiency and readiness. Within any functioning democracy, effectual public service at its very foundation is about public trust.² To successfully accomplish our military mission, continuing public trust is an absolute imperative.

The CFR/JER, Department of Defense Ethics Fundamentals, and Fiscal Responsibilities

“Ethics is knowing the difference between what you have a right to do and what is right to do.”
—Potter Stewart, U.S. Supreme Court justice

Department of Defense ethics, as a practical matter, are influenced and guided by a common rule set. The Code of Federal Regulations (CFR) and the JER² provide explicit standards regarding personal conduct related to federal employ-
ment. These rules detail institutional right and wrong behaviors, as well as identify areas where appearances of improprieties can reduce public trust and confidence. They embody a code of professional conduct detailing what Department of Defense personnel can and cannot do. These rules are not malleable, nor are they mere guidelines or simply suggestions.

The Department of Defense—the Ethics Counselor’s Sole Client

Oftentimes, the specific rules regarding Department of Defense ethics are not entirely intuitive, and personally striving to “be ethical,” although admirable in its own right, does not necessarily ensure one is accepting adhering to all of the applicable ethics rules. In other words, compliance with specific ethics rules is not necessarily the same thing as, in the abstract meaning, “being ethical.” Merely doing what a person thinks is right might not always be enough. Accordingly, to assist military and civilian personnel in relation to the many Department of Defense ethics rules and how they apply, designated attorneys are charged with providing, on behalf of the Department of Defense, both general and specifically-tailored ethics advice.

A Department of Defense employee appointed as an Ethics Counselor shall be an attorney. When providing ethics advice, our client is and remains the Department of Defense, never the individual counseled. To ensure objectivity, when an ethics counselor advises and counsels an individual commander or leader, the ethics advisor acts solely as a Department of Defense lawyer. The ethics advisor acts as a designated public official who, strictly on behalf of the Department of Defense, furnishes specific ethics compliance information. The ethics advisor provides only an “arm’s-length” legal opinion to the individual advised. It is an objective government-counsel advisory legal opinion that provides a Department of Defense interpretation of ethics rules as applied to the facts relating to an individual’s proposed conduct. The ethics advisor does not represent, or advocate for, the individual advised. Accordingly, although our ethics advice is usually individualized to the specific personnel we counsel, it is not protected by the attorney-client privilege and we must proactively and clearly so advise the recipient.

Ethical Ethics Counseling

“Ethics must begin at the top of an organization. It is a leadership issue and the chief executive must set the example.”

—Edward Hennessey Jr., Fortune 500 company CEO

J.P. Morgan, American financier and banker in the late 1800s and early 1900s, famously said, “I don’t want a lawyer who tells me what I can’t do. I hire a lawyer to tell me how I can do what I want to do!” This leadership philosophy, in relation to the utilization of legal counsel in business, admittedly also has some relevance in various areas of military law practice in direct support and furtherance of the operational mission. However, this philosophy has little to no application to proper ethics advice because the facts or proposed action might involve a potential inappropriate personal gain, benefit or perk to the individual advised. Ethics counselors are federal government officials, not lackeys.

In fostering and maintaining an effective organizational ethical culture and value system, most senior Department of Defense leaders do not even want to bend, let alone break, ethics rules. Most leaders appreciate that if one chooses to continually run close to and alongside the ethical sidelines, one eventually will step out of bounds. Accordingly, the majority of leaders sensibly do not wish to be anywhere near where the ethical boundary line has been drawn. It follows that no ethics counselor is ever doing any senior leader a favor by being an ethical Gumby. Instead, we as ethics counselors are to assist effectively a commander in the development of a credible ethical culture within the organization through the implementation of the commander’s ethics program. Consequently, we must endeavor always to provide honest, accurate, objective, unambiguous, timely, and consistent legal ethics advice. That is, ethical ethics advice.

Ethics counselors should be forward-leaning and strive to foresee potential problems. At times, an individual seeking ethics advice might not be completely forthcoming and provide you all the salient facts. Before a competent ethics counselor provides advice, the counselor frequently must first “peel back the onion” and expose the underlying layers in order to determine and verify all the actual facts. An accurate and complete representation of the relevant facts is vital to render any valid ethics opinion. With legal advice, one specific factual detail may be dispositive. The adoption of incomplete, shaded or wrong facts in an opinion gives an unwarranted credibility to an event or action, not only for the current year, but for future years as well. With incomplete or inaccurate facts, we can only provide incomplete and likely inaccurate ethics advice.

Consequently, when asked an ethics question, avoid providing an immediate “shoot-from-the-hip,” “gut-sense,” or “knee-jerk” yes or no. In regards to professional ethics advice, relying upon common sense only or making an informed guess based upon the limited facts immediately before you might not result in the right answer. Discover the relevant facts, research the applicable law and rules, and craft an accurate, objective and complete answer.

“Disinterested from ethics, leadership is reduced to management and politics to mere technique.”

—James MacGregor Burns, presidential historian

It is rarely if ever appropriate to engage in “legal gymnastics” and stretch ethics rules to the breaking point in an attempt to justify a perk or other personal benefit or a Department of Defense official. When a leader is personally advantaged due to receiving an unauthorized benefit or perk, it undercuts the leader’s moral authority which is essential and implicit to authentic and effective leadership.

In addition, when an ethics counselor gives dubious advice that purports to validate a questionable ethical practice, it encourages ethics advice forum-shopping. It promotes an unsound view that any ethical question can be legally justified within the rules to the direct personal benefit of the individual if one simply finds and asks the right acquiescent or complicit ethics counselor. Of further concern, if members of the command believe that almost every ethical issue can or will be legally justified by an ethics counselor, they will then be led to believe that ethics advice is unnecessary and, inevitably, will be less inclined to request it.
Advising the Ethically-Challenged

“Our government is the potent, the omnipresent teacher. For good or for ill, it teaches people by example. If the government becomes the law-breaker, it breeds contempt for law and invites every man to become a law unto himself.”

—Louis Brandeis, U.S. Supreme Court Justice

Whenever faced with a “risk-taking” or a potentially ethically-challenged leader or team member, we as ethics counselors should deftly explain the possible or likely consequences of non-compliance or ill-advised, unduly flexible and expansive interpretations of ethics rules. In order to avoid ethical violations, we want our leaders and team members to proactively seek out our advice. Be accessible, always.

“If ethics are poor at the top, that behavior is copied down through the organization.”

—Robert Noyce, inventor of the silicon chip

“An ethical person ought to do more than he's required to do and less than he's allowed to do.”

—Thomas Jefferson

Useful ethics advice is not merely the sterile recitation of a technical legal analysis. It is not limited to determining only whether a particular proposed action might be legally permissible. Depending upon the circumstances, an authorized gift may still be perceived reasonably as a de facto bribe or payola; an upgraded commercial airline travel seat or hotel room might be perceived reasonably as spend-

Do not ever set up a senior leader for failure by giving deficient ethics advice because you think it is what the leader “wants to hear.” Provide the correct advice that the leader “needs to hear.”

ing U.S. tax dollars extravagantly; or a commercial enterprise’s invitation to a Department of Defense senior leader to an expensive leisure event or extravagant dinner could be viewed reasonably as poorly disguised graft attempting to mask the central intent of the enterprise to garner access or influence illegitimately.

An ethics counselor should never ignore the appearance of impropriety which may accompany an event that, although potentially legal, should be avoided. When advising on ethical matters, an ethics counselor must provide a considered judgment of the potential for a negative public perception that could be generated by a leader’s participation in such an event. In ethics, where appearances are just as important as reality, events that can create appearances of impropriety are fraught with danger and could pave the way for subsequent ethical missteps, all with career-impacting ramifications to the doer.

To both the American public and a leader’s subordinates, per-
ceptions can credibly equate to reality. Accordingly, Department of Defense personnel should strive to avoid even the appearance of an ethical impropriety. Even if a particular course of action might be rationalized as meeting minimal Department of Defense ethical standards, if others could reasonably view the conduct as inappropriate, it still might be unwise or even patently stupid to do.

Ethical Failures by Leaders and Ethics Advisors

“Even the most rational approach to ethics is defenseless if there isn’t the will to do what is right.”

—Alexander Solzhenitsyn

As previously mentioned, over the past few years, our military has experienced dispiriting examples of failures in leadership involving ethical violations. Unethical is synonymous with unprincipled, unscrupulous, and corrupt. Ultimately, those who willfully violate Department of Defense ethics rules are fitly called “criminals.” Such regrettable cases have also, at times, involved attendant highly unfortunate and discouraging failures in the tendering of ethics advice. When a senior leader in our armed forces is implicated in an ethics scandal due to inaccurate ethics advice, the ethics counselor is then likewise culpable.

There are often reasons, other than simple incompetence, for the offering of erroneous ethics advice. Some incorrect “getting to yes” advice possibly involved an ethics advisor’s self-serving attempt to please or otherwise garner potential approval or favor from a senior officer. Some misguided or off-the-mark advice likely resulted from an ethics counselor’s subconscious rationalizations that a senior officer merited or was somehow entitled to an otherwise unauthorized gift, special privilege, or travel perk, or that such a personal benefit was expected or appropriate, due to that officer’s rank, status, or position. More likely, some misplaced ethics advice was provided due to an ethics advisor’s overly deferential unwillingness to speak truth to power or to ever advise “no” to a senior officer.

It is the unfortunate truth that in each of these situations, short-sighted ethics counselors failed to serve their respective commanders and leaders. Much more notably, they utterly failed to represent and serve their sole client, the Department of Defense. An ethics advisor’s role is to provide proper and accurate advice based upon the applicable facts and rules. Do not ever set up a senior leader for failure by giving deficient ethics advice because you might think it is what the leader “wants to hear.” Provide the correct advice that the leader “needs to hear.”

To be sure, ethical ethics counseling is not for the faint of heart who routinely seeks the path of least resistance and, despite the facts and rules, would reflexively aim to please the boss in each and every circumstance. As ethics counselors, we are charged with protecting the Department of Defense, our leaders and the rest of the Department of Defense team by providing correct advice consistently.

Model the Ethics Advice That You Give

“An ounce of practice is worth more than tons of preaching.”

—Mahatma Gandhi

Effective and ethical ethics counselors model the behavior they
advise. As ethical ethics counselors, we must never tacitly approve of any factual misrepresentation or engage in any institutional/corporate lying in attempts to manufacture compliance with ethics rules. That is not what “right” looks like.

“Every time we turn our heads the other way when we see the law flouted, when we tolerate what we know to be wrong, when we close our eyes and ears to the corrupt because we are too busy or too frightened, when we fail to speak up and speak out, we strike a blow against freedom and decency and justice.”

—Robert Kennedy

When an ethics counselor is apprised of improper conduct, the counselor has a professional duty to intervene proactively to provide the correct advice to senior leaders in order to set or maintain a proper ethical environment. This intervention may require a public statement by the senior leader or ethics counselor to ensure all members of the organization understand an activity or event was improper under our ethics rules.

Failure to do so engenders the appearance of selectivity in application of the rules or worse, the ethics counselor’s tacit approval of the inappropriate activity. Averting one’s eyes will simply generate or amplify an exceedingly faulty perception that

Whenever ethics are at issue, it is unquestionably better for any individual to take the proper initiative to ask for an ethics opinion. That is what “right” looks like.

one is likely better off by simply not asking for an ethics opinion on an issue. Only “if it becomes necessary after the fact, then beg for forgiveness, but do not start out limiting yourself by asking for permission…” This calculated view that ignorance is bliss is inherently flawed.

Whenever ethics are at issue, it is unquestionably better for any individual to take the proper initiative to ask for an ethics opinion. That is what “right” looks like. On a practical level and as a matter of preventive law, through complete, accurate, and ethical ethics advice, ethics counselors can substantially contribute to Department of Defense collective efforts in proactively guarding against any circumstances involving ethics in which the Department of Defense, our leaders, and team members would be displayed prominently and negatively within the media and to the American public.

**Fulfill Your Ethical Duty**

“Always do the right thing. This will gratify some people and astonish the rest.”

—Mark Twain

Ethical ethics counseling perfectly aligns with and is embraced wholly within a government attorney’s guiding principles of wisdom, valor, and justice. Wisdom encompasses knowing the law and how to adeptly apply it to the relevant facts. Valor is exemplified through citing the law, unabashedly, and even when unpopular. Justice is advanced by facilitating conformity to rightness in action and attitude.

Col. Joseph P. “Dutch” Biaiske, B.S., M.A., J.D., LL.M., is the Staff Judge Advocate, Third Air Force (3AF), Ramstein Air Base, Germany. He is the senior and principal legal advisor to the Commander of 3AF. Col. Biaiske is responsible for the administration of all military justice actions within the 3AF command that comprises over 30,000 U.S. Airmen. He provides legal support for 3AF headquarters and functional/technical military justice administration oversight of eight wing legal offices and four additional legal offices within the 3AF area of responsibility. Col. Biaiske served in the North Dakota Army National Guard as an Army Officer from 1986-1992, primarily in the combat arms Air Defense Artillery Branch. He served as law clerk to the Honorable Beryl J. Levine of the Supreme Court of North Dakota from 1991 to 1992. In 1992, Col. Biaiske was commissioned an Air Force Officer and designated an Air Force Judge Advocate. He has since served in a variety of base-level, Numbered Air Force, and joint/combatant-command legal positions. Col. Biaiske has also served in numerous operational and international law assignments. He deployed with the 82nd Airborne Division to Haiti during Operation Uphold Democracy ('94); deployed to the Balkans during Operations Joint Guard/Forge ('98); and deployed to Iraq during Operation Iraqi Freedom ('07).

**Endnotes**


4Joint Ethics Regulation (JER) DoD 5500.7-R. The JER supplements regulations issued by the U.S. Office of Government Ethics (OGE) at 5 C.F.R. § 2635. 5 C.F.R. § 2635 is the controlling regulation that the JER augments. The complete text of the JER and 5 C.F.R. § 2635 is available at www.defenselink.mil/dodoc/defense_ethics/index.html. See also, DOD’s supplement to the Standards of Conduct, found at 5 C.F.R. § 3601 et. seq. See also JER, Chapter 2, Section 2; and DOD Employee’s Guide to Standards of Conduct.

5JER § 1-212.

65 C.F.R. 2635.107(b); See also U.S. v. Schaltenbrand, 930 F.2d 1564 (11th Cir., 1991).

7For a recent egregious example of unethical conduct, review

*See Memorandum from Deputy Secretary of Defense to the Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, *et al.*, Subject: Ethics, Integrity, and Accountability, 21 Dec 2010:

Consider the appearance of your actions—whether they set the right example for peers and subordinates, and how they portray the Department in the eyes of the public. This is especially true for supervisors and managers, whom I expect to lead by example and whom I charge with creating an ethical culture in the workplace. We simply cannot tolerate ethical deviations or shortcuts.
learned from the long and somewhat eventful history of intelligence oversight may be fruitful. What has worked well? What has proved redundant or unduly subject to politicization?

The intelligence experience offers a fourth additional lesson. Homeland security is arguably the most legally intensive of the national security law fields. There are complex questions of constitutional law involving federalism, the military, privacy, and federal regulation of the private sector. It is no surprise that Northern Command has the largest staff judge advocate’s office. What’s more, many of these issues are new issues, for which there is no practice or precedent on which to call. That means that lawyers should not just advise on the substance and process of law. They should actively and aggressively appraise the implementation of law for unintended consequences and efficacy. As the DNI is required to report to the president and the Congress each year on the state of intelligence law, homeland security lawyers should identify any statute, regulation, or practice that impedes the ability of their agency to fully and effectively secure the nation. Likewise, policymakers and lawyers should take note from the intelligence experience – law can facilitate response, but legislation marks a beginning of the process, not its conclusion. Homeland security like intelligence ultimately depends on the human factor – leadership and the moral courage to face hard risks and make hard choices.

10 The National Security Lawyer

This book has considered national security law and process in the context of four security threats. First is the threat of attack by nonstate and state-sponsored or supported actors using terrorist means. Overseas, this threat is realized on a daily basis. Within the United States the threat is continuous, but intermittent. The threat of high-explosive attack, like car and truck bombs, targeted suicide bombings, or the sabotage of aircraft, is most likely to materialize. The threat of catastrophic attack with nuclear weapons has the greatest potential impact on our way of life and in terms of human cost. It is in relation to this threat in particular that we need to evaluate and test national security law and process, both because of the potential consequence and because of the focus the enemy has placed on this means of attack.

Second, U.S. constitutional values may ebb and wane in an endless conflict against state and nonstate actors engaged in acts of terrorism or posing the threat of terrorism. In light of the interminable nature of this threat, assertions of presidential authority made in extremis may become embedded in U.S. practice and law without a corresponding application of checks and balances. Left outside the reach of effective and independent mechanisms of appraisal, broad assertions of executive authority may in time diminish both the principles of law that define American life as well as the physical security at which they are directed.

Third, sincere policy differences, as well as those that are politically inspired, regarding the nature of the terrorist threat and the corresponding measure of response may result in a zero-sum compromise; that is, a diminution of security or a diminution of law, rather than contextual formulas that advance both at once. If the executive needs broad and rapid authority to engage in intelligence collection – as it does – the better course is not to limit the authority, for fear of misuse, but to increase the opportunities for meaningful internal and external appraisal. Such appraisal will deter misuse, but as importantly, encourage effective use. In this enduring conflict we may exhaust our resources or our principles in a manner that leaves us unwilling...
or unable to effectively address this century’s other certain crises, including the proliferation of weapons of mass destruction to unreliable state actors, the advent of pandemic disease, and environmental degradation and change.

This book has focused on the threat of terrorist attack because this is the threat that today drives the legal debate about the president’s constitutional authority. More generally, it drives the purpose and meaning of national security law. It will continue to do so. It is also the threat with the greatest potential to transform U.S. national security, in both a physical and a values sense. The importance of addressing other issues, such as conflict in the Middle East, totalitarian regimes, or pandemic disease, must not be overlooked. Each bears the potential to spiral beyond control resulting in catastrophe at home and overseas. Each of these issues warrants full consideration of the national security instruments and processes described in this book.

In each context, law and national security lawyers contribute to national security in multiple ways. First, the law provides an array of positive or substantive instruments the president may wield to provide for security. Second, the law provides procedural mechanisms offering opportunities to consider, validate, appraise, and improve policy, as well as ensure its lawful execution. These mechanisms include the horizontal separation of constitutional powers at the federal level, and the vertical separation of powers between the federal government and state government. They are found as well in statute and in internal executive directive.

The most effective means of appraisal are often found through informal practice. Informal contact allows participants to speak with a freedom not permitted or not often found when bearing the institutional mantle of an office or branch of government. Consider the difference in reaction between the counselor that sits down with the policymaker for a discussion and the counsel who requests the policymaker to put down in a memorandum everything that occurred. With informal practice the role of personality and friendship can serve to facilitate information exchange and the frank exchange of views.

Third, in the international context, law provides mechanisms to achieve U.S. national security objectives. This is evident in the context of maritime security, where U.S. law is pegged to an international framework, and effective security requires international as well as domestic participation. In the area of intelligence integration, bilateral and multilateral agreements, like the PSI and bilateral aviation agreements, provide essential mechanisms for identifying intelligence, sharing intelligence, and acting on intelligence.

Fourth, the law reflects and projects American values of democracy and liberty. Values are silent force multipliers as well as positive national security tools. As Lawrence Wright, the author of The Looming Tower, and others argue, jihadists like Osama Bin Laden offer no programs or policies for governance, no alternative to Western democracy. They offer only the opportunity for revenge. Rule of law is the West’s alternative to jihadist terrorism. Law, and respect for law, offers the structure of democracy, the opportunity for individual fulfillment regardless of sex, race, or creed, and a process for the impartial administration of justice. Sustained commitment to the rule of law in practice and perception will serve as a positive national security tool in curtailing recruitment of the next wave and generation of jihadists.

But law, like homeland security, is an incremental endeavor. It is dependent on sustained action, not rhetoric, and perceptions can be swept aside in a few ill-chosen moments. Law, like this conflict, requires sustained sacrifice and sustained support. Thus, divisive legal arguments should be eschewed, unless they are essential to security and there are no alternative means to accomplish the same necessary security end.

The law may contribute to national security in other ways as well. The law is a source of predictability. Through prediction, it becomes a source of deterrence. If the law is understood to permit the use of force, or the collection of intelligence, then allies and opponents alike may modulate their behavior accordingly.

Law can also be a source of calm and stability at times of crisis, guiding but not compelling decisionmakers to processes of decision that rapidly identify risks and benefits and fix accountability. Rapid decision can be obtained through secrecy and by truncating process; it can also be found through the expectation and practice that process provides. This is evident in the case of the military chain of command. This can be true with the president's national security processes as well.

The law is also a source of continuity. An enduring conflict requires enduring commitment, in values, funding, and sacrifice, and thus unity across party or factional transitions. Where essential policy is embedded in framework statutes, it is less subject to, but not immune from the vicissitudes of momentary political advantage or the policy pressures of immediacy. In a conflict marked by intermittent attacks over years, at least in the United States, law can insulate policy from the loss of public or even official attention. For example, where a tool is dependent on sustained funding and policy commitment, legal mandates can hold bureaucratic focus. And, where policy is embedded in law, intelligence and law enforcement operations may take greater risks knowing the authority for their actions is documented in law and not dependent on classified authorities or recollections of approval.

At the same time, there is much the law cannot do. Law and process provide an opportunity for success, but do not guarantee result. Leadership, culture, personality, and sometimes good luck are as important as law. A well-crafted emergency response directive does not compel first responders to climb the stairs of a burning building -- courage, leadership, and commitment do.

Law is a human endeavor that is dependent on the human factor. We are a nation of laws, but we are also a nation of men and women, or if you like a
nation of law and lawyers. It is men and women who write the law, interpret the law, and decide whether to uphold the law. Where national security is at stake, the human influence is manifest. "National security" necessarily involves the application of subjective values and not just security criteria. Further, as considered in Chapter 4, the law is as dependent on theory as it is on black-letter principle, and thus is dependent on human values and choice. Even where the law is clear, the facts rarely are, for the reasons articulated in Chapter 7. The application of fact to law, of intelligence to security, involves human judgment rather than the mechanical review of facts.

Law also involves moral courage. Field Marshal Slim, who served on the Western Front during the First World War and is considered one of the best commanders during World War II, compared physical and moral courage. He described moral courage as "a more reasoning attitude, which enables [a man] coolly to stake career, happiness, his whole future, on his judgment of what he thinks either right or worthwhile." Slim said,

I have known many men who had marked physical courage, but lacked moral courage. On the other hand I have seen men who undoubtedly possessed moral courage very cautious about taking physical risks. But I have never met a man with moral courage who would not, when it was really necessary, face bodily danger. Moral courage is a higher and rarer virtue than physical courage.1

Most lawyers will not have Field Marshal Slim's opportunity to test the comparative proposition. But they will have their moral courage tested. They will be tested sitting at a Principals Meeting when they have to decide whether, and how to speak up. They will be tested when they must step outside their personalities. loud, quiet, or in between, and step into a different role in order to apply the law more meaningfully. The quiet personality will be asked to make public presentations on behalf and in defense of the law. Sometimes the strong personality must sit down for the law, for example, at an interagency meeting where bureaucratic diplomacy may be the order of the day. But minutes later, in the face of the deputy secretary or national security advisor, the lawyer must have the courage to insist on attendance at a necessary meeting. In short, national security law is as contingent on the national security lawyer as it is on the law.

A. NATIONAL SECURITY LEGAL PRACTICE

In a constitutional democracy decisions are intended to be made according to law. That means that sound national security process must incorporate timely and competent legal advice. What form should that advice take?

In some cases, legal review is dictated by statute, as in the case of the Foreign Intelligence Surveillance Act, which requires designated officials, including lawyers, to certify requests for electronic surveillance or physical search before they are submitted to the FISA court. In other cases, the president has directed a specific process of legal review; for example, in areas historically prone to peril, such as covert action. However, the majority of legal advice within the national security process is not required by law or directive, but is the product of practice, custom, and the rapport, if any, between officials and their lawyers.

At the national level the daily participants are generally the same from administration to administration: the attorney general and deputy attorney general; the Office of Legal Counsel within the Department of Justice; and other agencies' general counsels, especially those at Defense, State, CIA, and DHS, as well as the chairman's legal advisor. Of course, in context, senior deputies and alter egos play an equivalent role.

Traditionally, lawyers for the president engaged in national security law have included the counsel to the president and the National Security Council's legal advisor. Practice varies as to the relative role and weight of each and the extent to which other White House lawyers, such as the deputy White House counsel, are involved in national security decision-making, if at all. Depending on administrations, and personalities, the role of the counsel to the vice president has ranged from a defining one to no role at all with respect to national security law.

Other lawyers play central roles as well. The judge advocates general of the military services, for example, are central players in the development of military law and legal policy as well as the application of the law of armed conflict. Within the Department of Justice, the assistant attorney general for national security, the head of the Office of Intelligence Policy and Review, the Office of Legal Counsel, and the assistant attorney general for the criminal division are all central players on issues of intelligence and counter-terrorism. Counsel at each of the intelligence community components and those engaged in issues of terrorism asset control and money laundering at Treasury also engage in daily national security practice. Each of these officials is supported by line attorneys who in many cases are the experts in their discipline and serve as the initial (and often) final point of contact for legal advice.

Each president, agency head, and commander will adopt his or her own approach to legal advice, ranging from active engagement with their lawyers and an understanding of the law to avoidance. Some officials do not seek legal advice unless the word "law" is mentioned and then only if it is mentioned four times in the subject line of a memo. Other officials view their lawyers as wide-ranging advisors, officials outside the policy process - non-stakeholders, and thus troubleshooters who may serve in capacity of counselor and not just legal advisors.

Officials and lawyers sometimes refer to lawyers "staying in their lane." But with national security there is rarely a street map. It is not always clear
where the lane begins or ends, and whether the intended road is a goat path or an informational superhighway. Some lawyers will operate on a defined track—litigators litigate, Office of Intelligence Policy and Review (OIPR) attorneys process FISA requests (among other things), the AECA lawyer reviews munitions list licenses. However, for more senior lawyers there are rarely set templates outside those dictated by law or directive for how to practice national security law. That means the individual lawyer will define the role as much as he or she will assume it. Moreover, policy officials will ultimately find those lawyers whose style and advice they trust regardless of individual assignments.

Application of national security law involves the rapid review and identification of legal issues embedded in policy options, policy decisions, and policy statements. At the NSC, for example, counsel traditionally coordinate the provision of advice to meetings of the Principals and Deputies Committees, among other tasks, and, where appropriate, attend such meetings to field questions and identify issues. However, this role appears to have varied in texture depending on whether the NSC staff are viewed as facilitators of interagency process or sources of rival legal advice to departmental general counsel. It also depends on the national security role assumed by the counsel to the president. In addition, NSC counsel provide internal legal advice to the president, national security advisor, and NSC staff as well as review and write memoranda to the president, issue spotting and discussing the legal issues raised. However, these roles are not defined in statute and are, outside the confines of certain narrow spheres, not defined in directive. Rather, these roles are defined by practice and the adoption or modification of past practice by successor officials.

Lawyers serving in defined billets are more likely to find continuity in the form and method of practice, but not necessarily in the substance of practice. For example, the assistant attorney general for the Office of Legal Counsel and his or her deputies generally provide constitutional advice to the executive branch and arbitrate interagency legal disputes, usually through promulgation of formal (often classified) legal memoranda. They are consulted, but are usually less active on daily issues of national security implementation and NSC policy development.

Likewise, line attorneys, as well as programmatic attorneys, are more likely to specialize in particular areas of law and find defined and generally accepted roles. This description might apply, for example, to a line attorney at the State Department who reviews export control licenses, or the attorney at the Treasury Department who reviews financial transactions with foreign states, or a Justice Department lawyer who reviews FISA applications. These lawyers play critical national security roles, but are less likely to address the breadth of national security issues identified in this book. Their lanes are relatively clear and defined.

In the Common Defense

The National Security Lawyer

In addition, lawyers serving as agency general counsel, or their equivalents, perform or oversee the performance of myriad tasks generally associated with lawyers, such as drafting legal documents, reviewing legislation, overseeing litigation, and addressing matters of budget, personnel, and contracting. Rule of law and respect for law are often defined by these tasks. Do the lawyers apply the ethics rules with reason, care, and rigor? Are legislative and public documents conducted in earnest? These everyday tasks help to define constitutional government, involving as they do the interplay between branches of government and the government and the public.

Harder to define is the role lawyers should take involving matters where there is discretion as to the style of practice, where the lawyer might have a choice between a proactive, active, or reactive role. In role-playing, personality can be as important as intellectual capacity and training. Not every lawyer is suited to a process of decision-making that can be rapid and is conducted under stress and often involves the application of law to uncertain or emerging facts. In this context, lawyers must know when to render their best advice and let go of an issue or when to hold an issue and request time for further review, or to buck the issue up the legal line. There is rarely time to double back for a second look. This may be difficult for lawyers who prefer the deliberative and careful speed of appellate work. It may also be difficult for lawyers who prefer practice areas oriented toward black-letter law and absolute answers. In short, national security practice requires a capacity to close on issues and make decisions, identifying nuance and cavets, if necessary.

National security practice also requires a capacity to compartmentalize work. This is true in a security sense. Lawyers operate under multiple constraints regarding what they can say and to whom based on the attorney-client, deliberative process, and state secrets privileges. (A sure way for a lawyer not to be in the right place at the right time is to garner a reputation for indiscretion.) However, by compartmentalization, I also mean an emotional and intellectual ability to move from one issue to another in rapid succession without getting stuck on just one issue. Policymakers must master this same skill. In contrast, subordinates assigned to specific issues are expected to devote their attention to a single policy issue and drive that issue up and down the chain of command.

As in other legal fields, national security lawyers should learn to subordinate matters of ego to the task of meaningfully applying the law. In doing so, they will have ample opportunity to learn the maxim that it is often the messenger who pays the price for the message. How common is the disapproving refrain, "Lawyers!" The refrain might be more aptly addressed—"Legislators!" "Democracy!" or "Benjamin Franklin!"—unless, of course, it is the lawyer who has delayed decision or diluted decision out of undue
caution or concern. Lawyers must also appreciate that while steady and
faithful application of the law is a hallmark of constitutional government,
in most bureaucratic and substantive contexts they are a supporting arm to
the policy process. Outside the Department of Justice, success is associated
with the policy and not the legal work that supports the policy.

Lawyers are also subject to having their advice tested, as they should.
That is part of the national security process and an essential part of inter-
and external appraisal. Does the lawyer understand the facts? Does the
lawyer understand the law? Has the lawyer distinguished between law and
legal policy? However, style varies. Where the stakes are high the distinc-
tion between understanding, testing, and bullying may be lost. Policymak-
ers have a duty to push. Policymakers do not become policy generals by
sitting back and waiting for events to unfold or opportunities to come their
way. Boot camp, it turns out, is sound training for national security lawyers.
National security lawyers will be tested and pushed, as they should be when
national security is at stake. The lawyers will know when a bad idea has
encountered a better idea and they must have the courage to adjust their
views; but they will also know when they have bent under pressure, know-
ing the difference between a good faith argument and an inability to hold a
line.

The practice of national security law, like many areas of law, requires
endurance. However, in private practice the client has usually come to the
counsel and now expects hard and constant effort. National security law
requires comparable effort, but a different kind of endurance. Lawyers are
not always invited into the decision-making room. This reluctance reflects
concerns about secrecy, delay, and "lawyer creep" (the legal version of "mis-
ion creep," whereby one legal question becomes seventeen, requiring not
one lawyer but forty-three to answer). Of course, decisionmakers may also
fear that the lawyer may say no to something the policymaker wants to do.
Rule of law often depends on the lawyer being in the right place at the right
time to render advice. This is achieved by reading agendas, attending staff
meetings, and ensuring that they and not the policymaker or the secretariat
define what it is the lawyer needs to see.

National security process is never designed to convenience the lawyer.
Sometimes it is specifically designed to avoid the lawyer. Endurance means
having fresh legs in the middle of the night as well as first thing in the
morning. Some officials will wait until the late night or the weekend to
move their memos, noting "not available" for a legal clearance. The lawyer
avoids such traps by meeting deadlines, negating silent consent, and where
necessary by laying out tripwires, alerting the executive secretary of issues
they need to see, sending timely e-mail prompting inclusion in discussions,
and meeting each policy staff member one-on-one to establish expectations
and confidence.

The National Security Lawyer

Most important, counsel should gain the support of the principal official
engaged. This is done by adding value to the process and articulating for
the decisionmaker why lawyers should have a seat at the table (or in the
Situation Room, along the wall). Counsel keeps that seat through effective
practice that is proactive, entailing the same zeal in overcoming legal and
bureaucratic obstacles as they show in identifying them. A lawyer engaged
at the advent of policy development is more likely to influence and guide
than one that clears the final memorandum to the decisionmaker, where
policy advisors have already committed to both the substance of decision and
means of execution. Moreover, if the lawyer waits for issues, or is perceived
as an obstacle rather than a source of value, the lawyer will find he or she
is only contributing to decisions where legal review is mandated and then
only as the last stop on the bureaucratic bus route.

Lawyers can advance the application of law in a number of ways. First, by
understanding national security process, counsel can better identify where
decisions are formed and made and thus where legal input is most useful.
Second, by understanding the military and intelligence instruments counsel
can better apply the law to fact. For example, military lawyers can hardly
apply the principles of proportionality, discrimination, and necessity to tar-
ggets without having an understanding of the weapons, munitions, and tactics
that inform judgments about necessity and proportionality. Likewise, counsel
addressing the use of force should understand the qualitative and quanti-
tative limits of intelligence, distinguishing between evidence, inference, and
intelligence in the process. Third, counsel must understand bureaucracy,
knowing when and how to provide advice in person, via memo, and through
e-mail, without losing sight that each written communication is a record no
matter how informal, and that tone and demeanor can get lost in e-mail.

Finally, counsel should master and proactively recommend legal methods
for overcoming bureaucratic inertia and resistance. Such methods include
(a) presidential directives, (b) agency directives, (c) interagency or intra-
agency memoranda of understanding, (d) lead agency designations, (e) the
conduct of exercises, (f) textual adjustments that defer or eliminate con-
cerns, or (g) just the force of personality or diplomacy. Concerns about the
deployment of armed forces in civil context might be addressed through
resort to any one of these methodologies or by textually limiting the scope,
service, or situation in which the forces might be used. Such limitations
might be put in the president's action memorandum, in the executive order,
or in the rules of engagement. Alternative process may work as well, such
as resorting to bimonthly meetings of the agency heads, in an effort to take
issues up and over bureaucratic obstacles, or holding weekly lunches of the
sort that Mr. Carlucci and Mr. Berger found effective.

Where lawyers are being used to dress policy disagreements up in deter-
native legal clothing—"my lawyer says this is illegal"—good legal process
can allow decisionmakers to focus on the policy issues at hand. Legal issues should be culled from policy agendas and intra- or inter-agency legal meetings held in advance to review options. This allows an opportunity to send issues up the legal chain rather than letting them linger, and possibly sidetrack deliberations. Moreover, just as policymakers forum shop for “can do” lawyers, or perhaps compliant lawyers, lawyers do the same, looking for lawyers who are problem solvers and do not shoot from the hip.

As in other areas of law, preparation is essential. This means reading agendas, consulting with relevant experts on an intra-agency and inter-agency basis, and taking issues up the legal chain of command in advance of meetings so that the lawyer can speak authoritatively when presented with the opportunity to do so. The opportunity may not come again.

Lawyers should also craft, and figuratively or actually, carry walk-about books to address national security issues as they arise. There is no excuse, for example, if the Northern Command staff judge advocate or counsel to the president does not have draft declarations "in the can" to address virtually every homeland security scenario. One purpose of tabletop exercises is to alert policymakers and lawyers to legal obstacles that lie ahead so that lawyers might find the means of circumnavigation before the crisis.

Preparation also entails educating the policymaker. Absent groundwork, the policymaker may respond at the moment of crisis by seeing the law only as something that allows or does not allow the policymaker to do what he wants. Contextual advice built on a foundation already laid is readily absorbed and accepted and will add greater value to the national security mission. A 3 A.M. conference call is no time to explain for the first time the principles of proportionality, necessity, and discrimination in targeting. Nor is the immediate aftermath of a natural disaster or terrorist attack the optimal time to explore for the first time the delicate legal policy issues raised by the deployment of U.S. military personnel in a civil context. In addition, the policymaker will understand in a live situation that the lawyer is applying “hard law” — specific, well established, and sanctioned — and not kibitzing on policy or operational matters.

Advance education also helps establish lines of communication and a common vocabulary of nuance between lawyer and policymaker before the crisis. A policymaker who hears a good brief on civil-military deployment will be sure his or her lawyer fully participates in any subsequent decisional process. In a large and layered bureaucracy, where the lawyer may be less proximate to the decisionmaker, and cannot count on immediate access, the teaching process is equally important in defining roles as well as legal expectations; however, it is more likely to occur through submission of written memoranda.

National security law also entails the application of legal policy; however, lawyers must take care to distinguish between what is law and what is legal policy. The identification of a preferred course as between lawful options is legal policy. The identification of a better argument among available arguments is legal policy. Identification of the long-term and short-term impact of legal arguments is legal policy. For example, will other states assert the same right to act as the United States asserts, and if so, what are the long-term costs and benefits of the United States asserting such authority? If a constitutional argument is legally available to the president, will it nonetheless generate a congressional or public response disproportionate to the benefits of using the argument?

The reality is that many national security law questions are not yes or no questions. Just as many national security policy decisions represent 51-49 judgments, legal judgments may be close calls; legal policy helps to identify the pros and cons of taking alternative positions. This is particularly the case where legal policy is national security policy as well; for example, where foreign reaction to U.S. legal choices may help or hinder alliances, or where reciprocal applications of law may harm U.S. national security.

Finally, lawyers, like policymakers, must return to appraise their work. Has the ground truth shifted in a manner that alters the legal basis for an action in either a permissive or restrictive manner? Has the president’s directive been implemented in the manner intended? Do the ROE provide adequate protection and flexibility for U.S. forces? Has process been implemented in a manner that facilitates or that impedes rapid decision or the identification of policy options?

In summary, the national security lawyer must consider not only the substance of the law but also the practice and process of law and the essential decisional skills that bear on the practice of national security law. In the end, however, most senior executive branch lawyers serve at the direction and sometimes discretion of the department counsel, department head, and ultimately the president. Chances are, if the policymaker is not satisfied with the manner, method, or substance of advice he will replace his counsel, seek his reassignment, or work around counsel to work with other lawyers. Whether he is satisfied will not only depend on the performance of the lawyer but also on whether they share common expectations of how to define the duties of the national security lawyer.

B. THE DUTY OF THE NATIONAL SECURITY LAWYER

Academics and practitioners sometimes define the roles and responsibilities of lawyers through identification of the client and the client’s interests. Thus, in private context, the ABA Model Rules of Professional Conduct state:

A lawyer must act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf.
It is the client who must decide critical questions of strategy and it is to the client to whom the attorney owes a duty of loyalty and confidentiality.

The client-based private model, however, is less apt in identifying and defining the responsibilities of the national security lawyer. To start, in government context, there are differing views on just who (or perhaps what) is the "client." Scholars and practitioners have identified both animate and conceptual candidates, including the president, the agency, the agency head, the public interest, and the Constitution. Consider that there are at least five possible and distinct facets to the president as client alone. At any given time the president may function as chief executive, party leader, commander in chief, the embodiment of the institution of the office of the president, or the president in his personal capacity. Each facet potentially represents distinct interests and responsibilities. While the national security lawyer certainly owes the president dedication and commitment as commander in chief, he does not necessarily owe the president as party leader the same zeal. Indeed, he may be legally barred under the Hatch Act from exercising any zeal at all.

In a related manner, there are differing perspectives, or models, on how national security lawyers should practice law, which reflect but are not necessarily determined by the identification of the "client." In the judicial model, for example, the lawyer is expected to render neutral detached views on the law, as a judge might, ultimately rendering a decision as to what the law is. The advisory model posits that the attorney will render advice on legally available options. The advocacy model, perhaps, is closest in paralleling the private model, with the attorney serving to guide the client to the client's preferred outcomes and then defending the client's actions. It might be said that with the judicial model the attorney works with both hands, presenting both sides of each issue. In the client-based or advocate model, the attorney works with one hand, finding a legal basis for what the client wishes to accomplish.

Such models bring structure to consideration of the practice of national security law and may serve as a point of departure in describing the duties of the national security lawyer. However, in the daily mix of practice, most national security lawyers do not relate their conduct back to specific theories of ethical responsibility and conflict of interest analysis, as a government or private practitioner might do in criminal practice. This reflects the nature of most national security practice. The provision of advice regarding the Foreign Assistance Act, for example, does not require identification of the client, but rather the competent official who can authorize use of the authority. This may vary depending on the section of law and internal agency process. When the assistant secretary asks whether the United States can provide aid, the question is not, who is the client? -- it is whether the Act authorizes such aid and, if so, subject to what substantive and procedural thresholds.

Likewise, judge advocates in the field do not ask, who is the client? -- they ask, which commander has the authority to issue the lawful order to attack?

Even where issues present what look like traditional private legal ethics questions, for example, in cases involving the waiver of a privilege, the question is not resolved through identification of the client -- for example, the agency or agency head -- but rather through knowledge of the substance of law and process. In the case of executive privilege the answer is the president. In the case of classified information the answer is found in some combination of the originating agency, the DNI, and the president. And in the litigation context, the answer may vary depending on who can ultimately speak for the government on the specific issue presented.

Moreover, attorneys need not resort to ethics or academic models to define their role, when so much of the role is already defined in law, and in particular in the Constitution. First, in Article II the president is charged with taking "Care that the Laws be faithfully executed." Second,

Before he enter on the Execution of his Office, he shall take the following Oath or Affirmation:

"I do solemnly swear (or affirm) that I will faithfully execute the Office of President of the United States, and will to the best of my ability, preserve, protect and defend the Constitution of the United States."

Third, Article VI requires that "all executive and judicial Officers, both of the United States and of the several States, shall be bound by Oath or Affirmation, to support this Constitution."13

As a matter of statute, government officials, including attorneys, also undertake an oath of office tied to the Constitution.

An individual, except the president, elected or appointed to an office of honor or profit in the civil service or uniformed services, shall take the following oath:

"I, ..., do solemnly swear (or affirm) that I will support and defend the Constitution of the United States against all enemies, foreign or domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God."

This section does not affect other oaths required by law. As is clear from the statutory text, the oath is not exclusive, but is applied in conjunction with other ethical obligations. Thus, in context, attorneys may well have to consider questions pertaining to the identification of the client. A judge advocate, for example, must adhere to his constitutional oath and to applicable bar codes pertaining to the representation of criminal law clients.
The point is that in the private context where academics and practitioners might reasonably debate to whom the attorney owes loyalty, the government attorney takes one oath and that is to the Constitution and not to a client. Further, that oath and the Constitution require faithful application of the law. That starts with faithful application of the Constitution, its structure and its substance, in the common defense of security and liberty.

Finally, the “client,” used here to identify the official with authority to decide an issue, as well as the role of the national security attorney, will vary in context. There are more than 40,000 lawyers in the government. Only a fraction of this number practice national security law. In each context, the “client” may be different. Moreover, within each setting the lawyer will (or should) play each role described above: advisor, counselor, advocate, and judge. The practice is also sufficiently contextual that the answer as to which role is appropriate is found not in identifying the client or a particular model of practice, but in the facts. The skill and art is in knowing when and how to play each role.

Consider the following hypothetical, presenting a preemption scenario likely to occur in the future. The president’s attorney is asked in the middle of the night to review a prospective target for a missile strike. For reasons of operational security, a “bigot list” is in place. It does not include the attorney general. The target is a suspected WMD weapons facility in a restricted country, but one with which the United States is nominally at peace. The facility is operating under cover as a legitimate commercial enterprise. The target is in play because of intelligence suggesting, but not confirming, that the plant is linked to an Al Qaeda affiliate.

For sound operational reasons, an up or down decision on attacking is needed within two hours, or sooner; to avoid the risk that the enemy will disperse extant WMD weapons. However, it turns out that at the staff level there is disagreement on whether the intelligence linking the target to terrorist actors or even clandestine activities is credible and persuasive. There are also differences of view as to whether additional methods of intelligence gathering may improve U.S. knowledge, although there is general agreement that the target is a hard target and that any disclosure of U.S. interest in the facility could lead to the rapid dispersion of existing WMD stockpiles (if any).

What is the role and the duty of the attorney, and is that role defined by identification of the client or application of a judicial, advocacy, or advisory model of practice?

In the advocate model, the attorney might determine that he or she will defend the president’s decision regardless of how the factual dispute is resolved, or for that matter whether it is resolved. Thus, the attorney might advise that so long as the president believes he is defending the country he has the legal authority to do so and counsel will support the decision under U.S. and international law.

The National Security Lawyer

In a judicial model, the attorney might ask additional questions. What is the potential for collateral consequences? And, what is the basis for the difference in intelligence opinion? He would then apply the law to the facts as they are known to determine whether a strike is lawful under U.S. and international law. To the extent the attorney believes the target is “unlawful” under U.S. law he would indicate so, and if necessary, advise the president that he could not in good faith approve the target.

Under an advisory model, the attorney might advise the president as to the legal standard and defer to the president’s judgment on the application of law to fact. Under the public interest model, the attorney might consider what is in the best interest of the United States or the public. Presumably this interest would revolve around getting the facts right, but also taking all measures necessary to defend the country, erring on the side of security.

The attorney should play all of these roles. First, under any rubric the attorney has a duty to resolve the factual ambiguity. Arguably, under an advocacy model, the attorney might sit back and defer to the president’s view of the law and facts and then defend both. However, it is not clear how such inaction would represent zealous or diligent representation. The president would still require knowledge of the facts and the law to faithfully execute his security functions. Moreover, under the advocacy model, even if the attorney were poised to validate the president’s judgment, he would still need to know the countermovements to better represent the president’s choice. Thus, the question is how best to do so in a manner that respects the role of the president as commander in chief and chief executive.

The hypothetical also illustrates the potential range of duties, functions, and choices the attorney might (and in my view should) address in a given scenario. The national security lawyer has a duty to guide decisionmakers toward legally available options. In performing this function in a timely and meaningful manner, the lawyer provides for our physical security. In doing it faithfully, based on honest belief on the application of law, he provides for the security of our way of life, which is to say, a process of decision founded on respect for the law and subject to law.

The hypothetical presents threshold questions of authority. Therefore, the attorney must consider whether the president has the constitutional authority to authorize the missile strike. As the president is also, in effect, approving a specific military target while authorizing the initial resort to force the attorney should run through a three-pronged substantive template:

(1) Does the president have the constitutional authority to use force, and is it subject to a statutory overlay? If so, must or should the president consult with the Congress, or notify the Congress in advance?
The attorney should also consider a procedural template:

(1) Who must authorize the use of force?
(2) Must the attorney general be informed? Should the attorney general be informed? If not, or if so, who must/should make that decision?
(3) Is the president aware of the factual dispute? If not, whose duty is it to inform him?
(4) Must the factual dispute be resolved before authorization may be given? If so, how can it be resolved in the timeline presented?

These questions present a mix of fact and law, law and legal policy, as well as substance and process. There are no textbook answers. There are clearly wrong answers. There are as well, as a matter of legal policy, preferred answers. One solution: the lawyer can identify the parameters of the factual dispute and ensure that they are framed and communicated within any decisional documents going to the president. But it is two in the morning! The president has already made his decision, without knowing that the facts are sliding. One solution: the president's lawyer can call the national security advisor and identify the problem and a solution — a conference call with the DNI, national security advisor, and the secretary of defense to determine if the facts are sliding or whether analysts are rehashing judgments already made at the top, without their knowledge. Does the DNI stand by the intelligence and intelligence judgment or not? And if there is any shift in fact or analysis, is the president and the military chain of command aware?

The scenario continues. With the input and concurrence of the attorney general, the DNI, and the secretary of defense, the president decides to authorize the strike. The lawyer now becomes advocate. He clears talking points for use with the Congress, the media, and foreign governments, conscious that the talking points, as opposed to the advice rendered in advance of decision, will shape outside perspectives on the validity of U.S. assertions of authority. As a matter of legal policy, will this be cast in the language of preemption, anticipatory self-defense, self-defense, or under some other rubric? In doing so, he considers what information if any can be disclosed in support of the intelligence link between the target and terrorism. He adds bullets on the legal basis for the strike, not as judge or advisor, reflecting the best arguments on both sides, but as advocate, presenting the arguments in support of action. Bigot list permitting, the lawyer ensures the State Department is generating an Article 51 report to the United Nations identifying the U.S. legal position as one of self-defense.

The strike occurs. The lawyer now shifts to the role of advisor appraising the process. What worked well and what didn’t work well? Could the factual dispute have been resolved through alternative process, or was it only identified and forced to the surface through the presentation of decision? Should the president retain case-specific decision authority over comparable strikes, or authorize such strikes in concept in the future and if so subject to what qualifications in policy, law, and legal policy? Is this a question of law, or of command preference that should be dictated by operational need and presidential style?

The hypothetical also illustrates the extent to which the application of national security law and process is dependent on culture, personality, and style. The president can direct legal review of his decisions, but if a national security advisor is not committed to such a review, it will not occur in a meaningful manner, if at all. The process would have failed if the lawyer did not make the call or if the national security advisor would not take the call. In short, it is not the presence of counsel at the NSC, the White House, or the Defense Department that upholds the law. It is the active presence of a president, a national security advisor, and department secretaries who insist on legal input in the decision-making process and lawyers who will place their integrity and careers on the line to provide it.

An indeterminate conflict, of indefinite duration, against unknown enemies and known enemies unseen will put uncommon strain on U.S. national security. It will also put uncommon strain on principles of liberty. If we meet this day's threats without destroying the fabric of our constitutional liberty it will be through the effective and meaningful application of national security law.

The sine qua non for broad national security authority is meaningful oversight. By oversight, I mean the considered application of constitutional structure, executive process, legal substance, and relevant review of decision-making — all of which depend on the integrity and judgment of lawyers. It is lawyers who will help us find the right combination of broad executive authority to defeat terrorism with the considered application of law before action and subsequent appraisal to protect our liberty. So whether one likes law or not, it is central to national security. Lawyers and not just generals will decide the outcome of this conflict.

Lawyers reside at the intersection where physical safety and liberty merge. In this role they are indispensable to good process and should feel a duty to advocate good process. Good process permits the faithful application
of the law and the accomplishment of the security objectives. In any given context, the pressure of the moment may encourage short-term thinking and the adoption of process shortcuts. The lawyer alone may be sufficiently detached from the policy outcome to identify the enduring institutional consequences of a particular course of action. So too, the lawyer alone may be familiar, and may feel an obligation to be familiar, with applicable written procedures. Process is substance if it means critical actors and perspectives are omitted from the discussion table.

Good process is not antithetical to timely decisions, operational timelines, or to secrecy. Process must find the right balance between speed and strength, secrecy and input. But process can always meet deadlines. There is no excuse for shortcuts. Process can be made to work faster and smarter. By example, if legal review is warranted, the attorney general alone can review a matter and, if need be, do so while sitting next to the president in the Oval Office.

Third, process should be contextual. The legal and policy parameters for responding to terrorism are different from those for responding to a Balkan crisis. Clandestine and remote military operations against a hidden enemy will dictate different decision processes than NATO air operations against fixed targets, as will the different political and policy parameters of both situations. One has to maintain situational awareness, to find the measure of process and approval that ensures law is applied in a manner that is faithful to constitutional, statutory, and executive dictates and that meets operational timelines. Therefore, there will always be some tension as to who should see what when.

Finally, lawyers support and defend the Constitution and not just the policies of their government. It is not clear how a president can faithfully apply the law without faithfully applying the constitutional principles identified in Chapters 3 and 4, including the separation of powers, and checks and balances. Constitutional faith recognizes that the Constitution is a national security document, which in the face of a WMD threat is appropriately read broadly and realistically. Constitutional faith also recognizes that liberty and the rule of law are national security values, which the Constitution is designed to preserve and to protect.

A definition of national security that includes constitutional values makes lawyers schooled in history, law, and ethics essential to the national security process. Being a lawyer in such a process is more than saying yes to a client's goals; it means guiding policymakers not just to lawful outcomes, but to outcomes addressing both aspects of national security by providing for security and preserving our sense of liberty. That is one reason this book places as much emphasis on the role of the lawyer as it does on the content of the law.

The National Security Lawyer

There are hard questions ahead in a time of homeland insecurity from which lawyers should not shy. Hamilton observed,

The violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions that have a tendency to destroy their civilian and political rights. To be more safe, they at length become willing to run the risk of being less free.

It is the national security lawyer's duty to alert policymakers to these tensions. The lawyer's duty is to show all sides to every issue while guiding policymakers and above all the president to lawful decisions that protect our security and our liberty. This is hardest to do when lives are at stake. But the Constitution was not designed to fail, to safeguard our security at the expense of our freedom, nor celebrate freedom at the expense of security. It is designed to underpin and protect us and our way of life. National security lawyers daily demonstrate how it can and must do both.

As a result, we should not begrudge democracy's adherence to law, but continue to find the best contextual process for its meaningful application. In war, and no more so than in addressing a threat where the terrorists' choice of weapons and targets may be unlimited, this means a substance, process, and practice of law that is both security effective and faithful to democratic values.

As Justice Brandeis reminded in Whitney,

Those who won independence believed that the final end of the state was to make men free to develop their faculties, and that in its government the deliberative forces should prevail over the arbitrary. They believed liberty to be the secret of happiness and courage to be the secret of liberty. The law depends on the morality and courage of those who apply it. It depends on the moral courage of lawyers who raise tough questions, who dare to argue both sides of every issue, who insist upon being heard at the highest levels of decision-making, and who ultimately call the legal questions as they believe the Constitution dictates and not necessarily as policymakers may want at a moment in time. We do not live in a moment in time. We and our children live in perilous times.
Ethical Issues of the Practice of National Security Law: Some Observations

CHARLES J. DUNLAP, JR.*

I. INTRODUCTION

In the twenty-first century national security law has become among the most challenging of legal disciplines in which to practice. This development has several causes, not least that the field embraces the most fundamental of all governmental functions: the Nation's security. As the Supreme Court insisted in Haig v. Agee,1 "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."

Before one examines the ethical conundrums occasioned by a national security law practice, the linkage of that discipline with developments in international law deserves comment. The tragedy of the 9/11 attacks and the resulting wars in Afghanistan and Iraq, not to mention the ongoing worldwide offensive against terrorists, have underlined not just the axiom of security being the most "compelling" of governmental interests, but also the reality that U.S. national security is inextricably intertwined with international events. In fact, one of the most important reasons for the rise of national security law has been the growing importance of law generally in international affairs.

That growth is, in large measure, a reflection of the phenomenon of globalization.3 This has significantly impacted the law because the dramatic

---

* Major General, U.S. Air Force (Ret.), J.D., Villanova University School of Law, 1975; B.A., St. Joseph's University, 1972. Deputy Judge Advocate General, U.S. Air Force, 2006-2010. Professor of the Practice of Law and Executive Director, Center on Law, Ethics and National Security, Duke University School of Law. This Article is based on a lecture presented as part of Ohio Northern University's Pettit College of 2012 Carhart Lecture Series on Legal Ethics, and some matters were previously discussed by the author in The Ethical Dimension of National Security Law, 50 S. Tex. L. Rev. 789 (2009).

2. Id. at 307 (quoting Aptheker v. Secretary of State, 378 U.S. 500, 509 (1964)).
3. The International Monetary Fund defines globalization as follows:

Economic "globalization" is a historical process, the result of human innovation and technological progress. It refers to the increasing integration of economies around the world, particularly through the movement of goods, services, and capital across borders. The term sometimes also refers to the movement of people (labor) and knowledge (technology) across international borders. There are also broader cultural, political, and environmental dimensions of globalization.

1057
increase in world commerce demands internationally accepted legal norms, instruments, and adjudicatory forums in order to work effectively. The *Economist* notes that we now live in “a world where barriers to the transfer of goods, expertise and people are coming down” and further observes that in “history, whenever cross-border commerce has flourished . . . so too have trade lawyers with broad horizons . . .”

The globalization of law, aroused by the globalization of commerce, has helped revolutionize the practice of international law, with real implications for a national security law practice. It is no surprise that Justice Sandra Day O’Connor uses martial language when she says that “understanding international law is no longer just a legal specialty; it is becoming a duty.”6 According to *U.S. News & World Report*. “Since the early 1990s, an explosion of international trade, the end of the Cold War, the rise of the Internet, and proliferation of international tribunals, and the new global war on terrorism have transformed the field of [international] law.”

The juxtaposition of the “new global war on terrorism” with “an explosion of international trade” is significant for the national security law practitioner because history repeatedly demonstrates that major developments in the economic sphere inevitably shape the conduct of war. Thus, everything from the development of agriculture (which permitted the rise of mass armies), to the industrial revolution (which enabled the mechanization of war), to the information age (whose technology permits

---

The term “globalization” began to be used more commonly in the 1980s, reflecting technological advances that made it easier and quicker to complete international transactions—both trade and financial flows. It refers to an extension beyond national borders of the same market forces that have operated for centuries at all levels of human economic activity—village markets, urban industries, or financial centers.

There are countless indicators that illustrate how goods, capital, and people, have become more globalized.

precision weaponry) illustrates how developments in the commercial sphere profoundly influence the way humans have fought.

It should not be surprising that the prominence the law—and lawyers—has achieved in the realm of globalized commerce parallels a similar growth in influence in national security matters, including the conduct of war. Senior military leaders acknowledge the new environment. General James Jones, the former commander of NATO forces, conceded that twenty-first century warfare is now “very legalistic and very complex,” requiring “a lawyer or a dozen.”\(^8\) In part, this “legalistic” aspect of warfare results from efforts of today’s adversaries to manipulate respect for the rule of law into something they can exploit. Professor William Eckhardt explains:

Knowing that our society so respects the rule of law that it demands compliance with it, our enemies carefully attack our military plans as illegal and immoral and our execution of those plans as contrary to the law of war. Our vulnerability here is what philosopher of war Carl von Clausewitz would term our “center of gravity.”\(^9\)

The evolving role of law—and lawyers—in national security matters post-9/11 has not been without controversy about the professional ethics of the discipline’s practitioners. Cynics, for example, argue that war is becoming “overlawyered.”\(^10\) More specifically, former Office of Legal Counsel (“OLC”) attorneys John Yoo and Jay Bybee were accused by the Justice Department’s Office of Professional Responsibility (“OPR”) of professional misconduct by “failing to provide ‘thorough, candid, and objective’ analysis in memoranda regarding the interrogation of detained terror suspects.”\(^11\)

A review by David Margolis, the Associate Deputy Attorney General, rejected the OPR findings and concluded that no professional misconduct, \(per se\), had taken place.\(^12\) He did so even though he found that there were “some significant flaws” in the memos,\(^13\) and that “Yoo and Bybee

---

12. Id. at 64–65.
13. Id. at 67.
exercised poor judgment by overstating the certainty of their conclusions and understating countervailing arguments.\textsuperscript{14}

As critics have pointed out, Margolis' conclusions are based on a standard employed by OPR that essentially requires proving more than what the American Bar Association ("ABA") Model Rules might require. David Luban maintains:

The OPR standard requires not just an ethics violation, but an ethics violation that the lawyer committed intentionally or in reckless disregard of the rules of conduct. In other words, OPR's framework requires proof of a guilty mental state over and above what the ethics rules themselves require.\textsuperscript{15}

Consequently, the cases of Yoo and Bybee, notwithstanding the exoneration of the two on ethics charges, do not provide much precedent useful to attorneys charged with ethics violations in the future, especially if they are judged on the more demanding standards of competence and candor expressed in the ABA Model Rules.\textsuperscript{16}

Beyond allegations of professional malfeasance, at least one national security law practitioner actually found himself criminally charged. Captain Randy Stone, U.S. Marine Corps ("USMC"), was one of the first persons criminally charged following the 2005 killing in Haditha, Iraq, of twenty-four unarmed civilians by U.S. Marines.\textsuperscript{17} Captain Stone was alleged to have failed to properly report and investigate the deadly incident.\textsuperscript{18}

Although the court-martial convening authority (then Lieutenant General James Mattis, USMC) later dismissed the charges, he did so not because he concluded no professional errors occurred, but rather because he did not believe that "any mistakes Captain Stone made with respect to the incident [rose] to the level of criminal behavior."\textsuperscript{19} Interestingly, Lieutenant General

\textsuperscript{14} Id. at 68.


\textsuperscript{18} See id.

Matti also observed that the lawyer and his fellow Marines "served in the most ethically challenging combat environment in the world."\textsuperscript{20}

While the battlefields of Iraq unquestionably present an "ethically challenging" environment, they are not the only places where the practice of national security law presents ethical difficulties. This Article does not purport to catalogue—let alone definitively resolve—every issue of professional responsibility a national security practitioner might face. It does, however, aim to illustrate at least some of the problems that are uniquely complicated by a variety of imperatives intrinsic to the national security law discipline.

Generally, the ethical behavior of lawyers, to include national security law practitioners, is governed by their particular licensing jurisdiction's code of professional responsibility. In most instances, these local codes draw upon the ABA Model Rules of Professional Conduct, which represent the legal profession's archetypal standards.\textsuperscript{21} The Model Rules do not, however, make many special accommodations for a national security practice,\textsuperscript{22} and that has caused some to question their utility in resolving the ethical issues that arise in a national security law practice.\textsuperscript{23} Nevertheless, they provide an appropriate starting point for discussion of this very important topic. Accordingly, this Article will survey the Model Rules and select a few of them to try to illuminate (through the examination of actual cases where possible) how they might apply in the national security law realm. This effort starts with an examination of the Preamble of the Model Rules.

II. THE MODEL RULES

\textit{a. Furthering the Public's Understanding, Confidence, and Participation in the Rule of Law}

As a public citizen, a lawyer should seek improvement of the law, access to the legal system, the administration of justice and the

\textsuperscript{20} Id.
\textsuperscript{21} See Model Rules, supra note 16.
\textsuperscript{22} Many government lawyers are required to abide by the McDade Amendment, Ethical Standards for Federal Prosecutors Act and the Citizen's Protection Act (also known as the "McDade Amendment") as implemented by the Ethical Standards for Attorneys for the Government, 28 C.F.R. § 77.1 (2012). These standards generally make a government attorney "subject to State laws and rules, and local Federal court rules, governing attorneys in each State where such attorney engages in that attorney's duties, to the same extent and in the same manner as other attorneys in that State." 28 U.S.C. § 530B (2011).
quality of service rendered by the legal profession... In addition, a lawyer should further the public’s understanding of and confidence in the rule of law and the justice system because legal institutions in a constitutional democracy depend on popular participation and support to maintain their authority.24

This excerpt from the Preamble to the Model Rules expresses what one might have thought, prior to 9/11, was a rather uncontroversial responsibility of a legal professional—to promote the rule of law whenever and wherever one could. However, in Holder v. Humanitarian Law Project,25 the Supreme Court essentially endorsed the government’s ability to prohibit the advancing of “the public’s understanding of and confidence in the rule of law and the justice system[,]” at least insofar as specific groups are concerned.26

Humanitarian Law Project involved a statute that criminalizes “material support” (to include “training,” “services,” and “expert advice or assistance”) to certain designated terrorist organizations.27 The Secretary of State had designated the Partiya Karkeran Kurdistan (“PKK”) and the Liberation Tigers of Tamil Eelam (“LTTE”) as terrorist organizations.28

What the nongovernmental organizations who were parties to the case sought to provide appears to be exactly what the Model Rules seem to encourage, that is, “train[ing] members of [the] PKK on how to use humanitarian and international law to peacefully resolve disputes”; “teach[ing] PKK members how to petition various representative bodies such as the United Nations for relief”; “train[ing] members of [the] LTTE to present claims for tsunami-related aid to mediators and international bodies”; and “offer[ing] their legal expertise in negotiating peace agreements between the LTTE and the Sri Lankan government.”29

The Court concluded that such activities could be prohibited consistent with the First Amendment.30 In rationalizing its view, it conjured up a variety of questionable theories. For example, it claimed that training to use law to peacefully resolve disputes might enable a “broader strategy to promote terrorism.”31 The Court hypothesized that the “PKK could, for example, pursue peaceful negotiation as a means of buying time to recover

25. 130 S. Ct. 2705 (2010).
29. Id. at 2716.
30. Id. at 2731.
31. Id. at 2711.
from short-term setbacks, lulling opponents into complacency, and ultimately preparing for renewed attacks.\textsuperscript{32}

Many scholars find the decision perplexing and wrong. For example, one First Amendment expert, David Goldberger, calls \textit{Humanitarian Law Project} "an incredibly broad ban on assistance to groups listed as terrorist groups, even where the assistance might have the effect of facilitating the abandonment of terrorism.\textsuperscript{33}" Even more inexplicable is the Court's reasoning in justification of the ban introducing extremist organizations to the rule of law. According to the Court, a "foreign terrorist organization introduced to the structures of the international legal system might use the information to threaten, manipulate, and disrupt. This possibility is real, not remote.\textsuperscript{34}

It is surprising that the Court would have so little confidence in the ability of various legal institutions to appropriately handle those that seek to "threaten, manipulate, and disrupt." Robust legal systems, such as that of the U.S., can deal with exactly that kind of person, and most develop rules and procedures to do so effectively. What is the alternative? History shows that extremist organizations can be pacified by integration into political and legal systems—the evolution of the Irish Republican Army being one example.\textsuperscript{35} Absent the incorporation of warring groups into the political process in accordance with the rule of law, it is difficult to conceive how some conflicts can be resolved. Training about the legal system and advice as to how to access it, along with efforts to further the understanding of and confidence in the rule of law and the justice system, as suggested by the Model Rules Preamble, would seem to be indispensable to such efforts; yet \textit{Humanitarian Law Project} largely precludes that, at least for certain groups.

Although \textit{Humanitarian Law Project} might be read as an unfortunate disparagement of the efficacy of the law to be an engine for dispute resolution, it is important for national security practitioners to keep in mind that the Court was not advocating a position, but rather merely ruling on the constitutionality of a statute. Still, the national security law practitioner should continue to try to advance—where permitted by the law—the use of legal means and institutions to resolve conflicts. However bitter and caustic

\textsuperscript{32} Id. at 2729.

\textsuperscript{34} \textit{Humanitarian Law Project}, 130 S. Ct. at 2729.

legal battles may be, they are always preferable to the ones marked by actual bullets and blood.

b. The Role of the Courts

*The legal profession is largely self-governing... [U]ltimate authority over the legal profession is vested largely in the courts.*

The idea that the "legal profession is largely self-governing" and that the "ultimate authority over the legal profession is vested largely in the courts" can be troubling in the national security setting, as the courts very often take a hands-off approach to national security issues. For example, with respect to the military dimension of national security affairs, the Supreme Court declared in *Gilligan v. Morgan* that:

"[I]t is difficult to conceive of an area of governmental activity in which the courts have less competence. The complex subtle, and professional decisions as to the composition, training, equipping, and control of a military force are essentially professional military judgments, subject always to civilian control of the Legislative and Executive Branches."

Courts very often seize upon an array of theories to avoid involvement in cases that raise national security matters. In many instances they halt the legal process by relying upon the "political question" doctrine, the "state secrets" theory, or standing. On other occasions, deference to the executive branch effectively ends litigation before the merits have been discussed.

36. MODEL RULES, supra note 16, Preamble and Scope, ¶ 10. The full paragraph reads:

"The legal profession is largely self-governing. Although other professions also have been granted powers of self-government, the legal profession is unique in this respect because of the close relationship between the profession and the processes of government and law enforcement. This connection is manifested in the fact that ultimate authority over the legal profession is vested largely in the courts."

37. Id.
38. 413 U.S. 1 (1973).
39. Id. at 10.
40. SPE STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 123 (5th ed. 2011).
examined. Indeed, Professor Stephen Vladeck contends that as of May 2012, there have not been any successful lawsuits “arising out of post–September 11 U.S. counterterrorism policies alleging violations of plaintiffs’ individual rights.” Professor Vladeck argues that a “national security canon” has arisen that effectively leaves those harmed by governmental action related to national security without legal recourse.

The judiciary’s use of these doctrines can have the effect of shielding the activities of lawyers from the scrutiny the courts might otherwise give their behavior. As a Harvard professor and former government attorney, Professor Jack Goldsmith, has noted, “[o]ften when an Executive Branch lawyer advises a client on a national security matter, their advice takes place in secret without a dissenting opinion or appellate review. This is a situation fraught with the possibilities of mistakes.” Thus, while the courts may well have “ultimate authority” over the professional conduct of attorneys, absent the transparency into their activities that litigation provides in other contexts, they simply cannot exercise that authority in a meaningful way.

A good example of the mischief that can result is found in the case of U.S. v. Reynolds, which has become accepted as the seminal case for the state secrets doctrine. This case arose out of a 1948 Waycross, Georgia, crash of a B-29 bomber carrying out tests on then advanced—and classified—electronic equipment. During discovery in a suit for damages by the relatives of the civilian victims (Radio Corporation of America employees who were aboard the ill-fated plane), the plaintiffs sought a copy of the Air Force’s accident investigation. The Government, employing rather ambiguous affidavits, denied the request, implying that classified information would be compromised by the report’s disclosure, and formally asserted that the report was privileged. Even the trial judge was denied access to it.

46. Id.
48. 345 U.S. 1.
49. See id.
50. Id. at 2–3.
51. Id. at 3.
52. Id. at 3-4.
Scholar Louis Fisher asserts that there "was a reason for the government to withhold the accident report from [the trial judge]." According to Fisher, it was not secrets that would be compromised; rather, the "report revealed clear negligence on the part of the Air Force, which had not installed heat shields and had failed to brief the civilian engineers before the flight on the use of parachutes and emergency aircraft evacuation." Not knowing what the report actually said, the Supreme Court upheld the government's position, finding that "when the formal claim of privilege was filed by the Secretary of the Air Force, under circumstances indicating a reasonable possibility that military secrets were involved, there was certainly a sufficient showing of privilege to cut off further demand for the documents."

The story does not, however, end there. In the year 2000, a daughter of one of the civilians killed in the crash discovered the declassified accident report for sale on the Internet. Subsequent examination of it confirmed that no classified information or equipment had been involved in the crash, and the plaintiffs sought to reopen the case based on the apparent fraud on the court. However, "[d]espite this showing of apparent government misconduct" the Supreme Court eventually denied a coram nobis petition for further review. In subsequent litigation, the plaintiffs were "denied relief because they were unable to show that government officials in 1953 had committed intentional fraud on the court."

Nevertheless, the Reynolds opinion has been severely criticized. Fisher argues:

The Supreme Court in Reynolds accepted at face value the government's assertion that the accident report and survivors' statements contained state secrets. That assertion was false. By accepting the government's claim and by not examining the

55. Id.
58. See id.
59. DYCUL, supra note 40, at 158 (citing In re Herring, 539 U.S. 940 (2003)).
60. Id. (citing Herring v. United States, 424 F.3d 384 (3d Cir. 2005), cert. denied, 547 U.S. 1123 (2006)).
documents, the Court appeared to function as an arm of the executive branch and failed to exercise independent judgment.\footnote{61}

As it happens, the state secrets privilege has recently come under scrutiny, as some in Congress believe the privilege is being abused.\footnote{62} Accordingly, legislation is being introduced designed "to counter federal judges who routinely accept the government’s privilege assertion on face value without any inquiry, sometimes without viewing any classified material to support the government’s position."\footnote{63}

It is impossible at this point in time to really understand the thinking of the government lawyers involved in the \textit{Reynolds} case, and to rationalize—consistent with the Model Rules—how they justified their conduct, which suggests, at a minimum, a lack of "candor."\footnote{64}

In any event, \textit{Reynolds} underlines the importance, as the ABA Preamble says, of the self-governing character of the legal profession.\footnote{65} Given the nature of national security issues, we cannot expect the courts to always exercise oversight and authority contemplated by the Model Rules, if for no other reason than the opaque character of much national security law litigation. In the end, for the national security law practitioner especially, compliance with ethical standards necessitates individual lawyers’ "self-governing."

c. The Lawyer as a Zealous Advocate

\textit{As advocate, a lawyer zealously asserts the client’s position under the rules of the adversary system.}\footnote{66}

---

63. \textit{id.}
64. See \textit{MODEL RULES}, supra note 16, R. 3.3
65. See \textit{id.}, Preamble and Scope, ¶ 10
66. \textit{id.} ¶ 2. The full paragraph reads as follows:

As a representative of clients, a lawyer performs various functions. As advisor, a lawyer provides a client with an informed understanding of the client’s legal rights and obligations and explains their practical implications. As advocate, a lawyer zealously asserts the client’s position under the rules of the adversary system. As negotiator, a lawyer seeks a result advantageous to the client but consistent with requirements of honest dealings with others. As an evaluator, a lawyer acts by examining a client’s legal affairs and reporting about them to the client or to others.

\textit{id.}
The Preamble speaks to a cardinal—and indispensable—responsibility of lawyers: zealous representation.\textsuperscript{67} Importantly, the Model Rules juxtapose the lawyer’s function as an advocate among other functions that the lawyer may serve in the context of representation. Though sometime misunderstood, this requirement for zealous advocacy does not mean that a lawyer must, or even can, do anything, anytime, that the client desires. As Justice Sandra Day O’Connor maintains, “[t]he hardest thing you must accept as an ethical, moral lawyer is that it is not your job to win for your client at all costs.”\textsuperscript{68} The case of Lynne Stewart is an example of a national security case where the attorney in question lost sight of Justice O’Connor’s admonition, and suffered for it.

Ms. Stewart was a self-described “radical human rights attorney”\textsuperscript{69} with a “reputation for defending unpopular clients and causes.”\textsuperscript{70} One of those clients was Omar Abdel Rahman, the “blind Sheik” who was convicted of various terrorism-related offenses including plotting to blow up the World Trade Center.\textsuperscript{71} As part of her representation, Ms. Stewart was required to agree to “special administrative measures” (“SAMs”) in order to get access to her imprisoned client.\textsuperscript{72} Among other things, these SAMs prohibited her from using her “meetings, correspondence or phone calls with Abdel Rahman to pass messages between third parties (including, but not limited to, the media) and Abdel Rahman.”\textsuperscript{73}

In 2005, Ms. Stewart was tried for several offenses arising out her representation of Rahman, including violating the SAMs by smuggling messages from Rahman to an Egyptian militant group, al-Gama’a, mostly about a ceasefire that the group had declared with regard to its violent efforts to overthrow the Egyptian government.\textsuperscript{74} In her defense Stewart insisted that she was merely acting “zealously” for her client. Convicted and sentenced to twenty-eight months in prison, Stewart defiantly declared that she “can do that [prison term] standing on [her] head.”\textsuperscript{75} In addition, when asked if she would do anything differently, she replied, “I don’t—I’d like to think I would not do anything differently . . . . I made these decisions

\textsuperscript{67} See id.
\textsuperscript{69} \textit{About, Justice For Lynne Stewart} (May 30, 2010), http://lynnestewart.org/about-lynnne/.
\textsuperscript{72} U.S. v. Stewart, 590 F.3d 93, 100 (2d Cir. 2009).
\textsuperscript{73} id. at 100.
\textsuperscript{74} U.S. v. Stewart, 686 F.3d 156, 162 (2d Cir. 2012).
\textsuperscript{75} id. at 165.
based on my understanding of what the client needed, what a lawyer was expected to do… I would do it again. I might handle it a little differently, but I would do it again.”

On appeal, Stewart reiterated her claim that she had been simply acting “zealously” to represent her client. However, the court rejected this contention, finding that

the jury had a reasonable basis on which to disbelieve this, and to “disbelieve that zealous representation included filing false affirmations, hiding from prison guards the delivery of messages to Abdel Rahman, and the dissemination of responses by him that were obtained through dishonesty.” Moreover, even if Stewart acted with an intent to represent her client zealously, a rational jury could nonetheless have concluded that Stewart simultaneously acted with an intent to defraud the government. A genuinely held intent to represent a client “zealously” is not necessarily inconsistent with criminal intent.

In fact, the appeals court would not affirm the sentence, returning it to the trial court for further consideration because the appellate judges could not “conclude that the mitigating factors” were sufficient to justify the original twenty-eight-month sentence “in light of the seriousness of her criminal conduct, her responsibilities as a member of the bar, and her role as counsel for Abdel Rahman.”

In a stunning turn of events, the trial court re-sentenced Stewart to ten years, the trial judge finding that the original sentence was not adequate because, among other things, she “abused her position as a lawyer.” That sentence was affirmed on appeal, as the judges ruled that not only was it lawful to consider Stewart’s post-conviction statements of bravado in the re-sentencing, but also that she

persisted in exhibiting what seems to be a stark inability to understand the seriousness of her crimes, the breadth and depth of the danger in which they placed the lives and safety of unknown

---

76. Id.
78. Id at 99.
innocents, and the extent to which they constituted an abuse of her trust and privilege as a member of the bar.  

In a pre-sentencing letter to the trial judge, Stewart gave an inkling of what may have been her key shortcomings.  

She spoke of seeing her job as a lawyer as that of “caring for the whole client,” to include “giving them money for food or their families,” and “visiting them on holidays”—activities beyond the usual professional responsibilities, and problematic ones in an era of sophisticated and exploitative international terrorists.  

Stewart indicated that she believed that “her stature in the legal community[,]” along with what she implies was general acceptance by the government of her way of practice in prior cases, would somehow exempt her from being viewed as having broken the law in the Rahman case.  

Perhaps most importantly, she admitted that “representing this convicted terrorist was still uncharted territory in the years 1997–2001” and that “what might have been legitimately tolerated in 2000–2001, was after 9/11, interpreted differently and considered criminal.”  

Clearly, the idea that terrorism and other national security cases are “different” and viewed with the utmost seriousness is a lesson that all lawyers would do well to internalize from the Lynne Stewart case. It is another manifestation of the precept that government has no more compelling interest “than the security of the Nation,” and that fact may well operate to diminish tolerance for behavior that might otherwise be excused.

d. Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.  

Competence for the national security law practitioner can be quite challenging. Almost by definition, national security matters are not the stuff

80. Stewart, 686 F.3d at 181 (emphasis added).
82. Id.
83. Id.
84. Id.
86. Model Rules, supra note 16, R. 1.1.
of most civilian experience. A contracts lawyer may have personal experience in buying a home or car that may familiarize him or her with issues arising in a similar transaction by a client. Contrast that with the national security law practitioner who may find himself or herself deliberating over a decision to kill another human being, or hundreds. Furthermore, some tasks may require considerable technical knowledge in order to utilize complex equipment in command centers, or to understand the weapons, warfare, and warriors of the national security discipline. Accordingly, specialized training is indispensable in order to function effectively, especially where high-technology weaponry is involved.87

The consequences of a lack of training can be serious. The case of Captain Randy Stone, the Marine lawyer accused of failing to properly report and investigate the Haditha incident, is instructive.88 Although he was “responsible for handling investigations and training Marines in the military’s laws of war,” Stone said “he received almost zero training for his job before joining the battalion in Iraq in September 2005.”89

National security law clients may have very high expectations about what they want a lawyer to understand about this “business.” Lieutenant General Michael C. Short, USAF (Ret.), who commanded air operations against Serbia90 in the 1990s, advised:

I would give an up-and-coming young operational lawyer wearing the uniform in defense of this country [the following advice:] Understand what your commander is up against. Understand and participate in the development of his rules of engagement. Understand what special instructions he is providing as supplemental to his rules of engagement, to his troops in field, or his men and women at sea, or his men and women in the air.91

87. See, e.g., Charles J. Dunlap, Come the Revolution: A Legal Perspective on Air Operations in Iraq Since 2003, in ISRAEL YEARBOOK ON HUMAN RIGHTS 141 (Yoram Dinstein ed., 2010), and reprint-
88. See McChesney, supra note 17; Press Release, supra note 19.
91. r02072000.pdf.
91. Lieutenant General Michael Short, USAF (Ret.), Operation Allied Force from the Perspec-
tive of the NATO Air Commander, in 78 U.S. NAVAL WAR COLLEGE, LEGAL AND ETHICAL LESSONS OF NATO’S KOSOVO CAMPAIGN 19 (Andru E. Wall ed., 2002) [hereinafter Operation Allied Force],
A national security law practitioner must, in many instances, have a deep enough level of understanding of the means and methods of national security activities to be able to offer lawful alternatives when possible. Offering timely alternatives is an indispensable aspect of this kind of practice, and is a quality that can earn the trust of the client.

When national security law practitioners demonstrate authentic competence, “client” commanders have greater faith in them, and will more readily incorporate them into the decision-making process. When that occurs, real dividends result. For example, when a Human Rights Watch analyst told the New York Times, in 2008, that the Air Force had “...all but eliminated civilian casualties in Afghanistan”\textsuperscript{92} in strikes that are a product of the deliberate planning process, the paper also pointed out that “Air Force lawyers vet all the airstrikes approved by the operational air commanders.”\textsuperscript{93}

Again, few things are more important for a “competent” national security law practitioner than a comprehensive and in-depth knowledge of not just the law, but also the “client” and his or her very unique “business.”

e. Special Conflicts of Interest for Former and Current Government Officers and Employees

[A] lawyer who has formerly served as a public officer or employee of the government . . . shall not otherwise represent a client in connection with a matter in which the lawyer participated personally and substantially as a public officer or employee, unless the appropriate government agency gives its informed consent, confirmed in writing, to the representation.\textsuperscript{94}


\textsuperscript{93} \textit{Id.}

\textsuperscript{94} MODEL RULES, supra note 16, R. 1.11. The full paragraph (and the following paragraph) states:

(a) Except as law may otherwise expressly permit, a lawyer who has formerly served as a public officer or employee of the government:
(1) is subject to Rule 1.9(c); and
(2) shall not otherwise represent a client in connection with a matter in which the lawyer participated personally and substantially as a public officer or employee, unless the appropriate government agency gives its informed consent, confirmed in writing, to the representation.
This is an area of the Model Rules that most involves the civilian sector, and particularly those who have previously served in government. It can ensnare even very highly respected and knowledgeable lawyers. An illustrative example with a national security law dimension is the case of Abraham D. Sofaer, a still much-admired and valued lawyer.\textsuperscript{95}

Sofaer was the Legal Advisor to the State Department from 1985 to 1990.\textsuperscript{94} In 1988, a bomb exploded on Pan Am flight 103 over Lockerbie, Scotland, killing 270 people, including 189 Americans.\textsuperscript{97} A Libyan intelligence agent was later convicted for his part in what was determined to be one of the worst acts of state-sponsored terrorism in recent years.\textsuperscript{98} In 2003, Libya, as a result of pressure from international sanctions, accepted “responsibility for the actions of its officials and [agreed to] payment of appropriate compensation to the victims’ families.”\textsuperscript{100} The compensation was reported to amount to $1.5 billion and its payment “clear[ed] the way for the full normalization of relations between Washington and Tripoli.”\textsuperscript{100}

After he left government and entered private practice, Sofaer undertook the representation of “the government of Libya in connection with criminal

(b) When a lawyer is disqualified from representation under paragraph (a), no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter unless:

(1) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and

(2) written notice is promptly given to the appropriate government agency to enable it to ascertain compliance with the provisions of this rule.

(c) Except as law may otherwise expressly permit, a lawyer having information that the lawyer knows is confidential government information about a person acquired when the lawyer was a public officer or employee, may not represent a private client whose interests are adverse to that person in a matter in which the information could be used to the material disadvantage of that person. As used in this Rule, the term “confidential government information” means information that has been obtained under governmental authority and which, at the time this Rule is applied, the government is prohibited by law from disclosing to the public or has a legal privilege not to disclose and which is not otherwise available to the public. A firm with which that lawyer is associated may undertake or continue representation in the matter only if the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom.

\textsuperscript{95} Mr. Sofaer is currently the George P. Shultz Senior Fellow in Foreign Policy and National Security Affairs at Stanford University’s Hoover Institution. Abraham D. Sofaer, HOOVER INSTITUTION, http://www.hoover.org/fellows/10685 (last visited Aug. 28, 2012).

\textsuperscript{96} See id.


\textsuperscript{98} id.


and civil disputes and litigation arising from the [Pan Am] bombing. As a result, the Board on Professional Responsibility ordered Soffer to receive an informal admonition for having violated Rule 1.11(a) of the District of Columbia Rules of Professional Conduct by accepting employment "substantially related" to a "matter" in which he participated personally and substantially as the Legal Advisor for the State Department.

In his defense, Soffer vigorously contested the precise meaning of the various terms in the rule, and offered several other explanations justifying his actions. However, the District of Columbia Court of Appeals adopted the Board report. In that report it was emphasized that it found a violation of the rules not because Soffer "undertook to represent an unpopular client" or because of "the appearance of impropriety that caused public condemnation of Respondent's private representation of Libya", rather, the Board

[D]id not believe that [the rule] allows a government lawyer to be briefed in the course of his official duties about a particular, sensitive investigation into a discrete event, so that he can provide legal advice, thereby learning important confidential information, provide substantial and personal legal assistance concerning the government's efforts, then leave the government and represent a suspect in the same investigation.

The court also found Soffer's activities "personal and substantial" and noted that they did not become "insubstantial" simply because "the legal judgment was easily arrived at or because the government subsequently concluded that Pan Am's theory of government complicity was unsupported." Finally, the court concluded that, while it may be possible for a former government lawyer to "limit the objectives of a representation with client consent" so as to avoid conflict (and emphasized that it did "not question the sincerity of respondent's belief that the representation could be insulated, factually and ethically, from the investigation and diplomatic efforts of which he had been part"), it nevertheless found the efforts to do so in this instance were inadequate.

102. Id. at 630.
103. See id. at 627–28.
104. See id. at 626.
105. Id. at 651–52.
106. Soffer, 728 A.2d at 651–52.
107. Id. at 627.
108. Id. at 628. See also Opinion 343: Application of the "Substantial Relationship" Test When Attorneys Participate in Only Discrete Aspects of a New Matter, DC BAR.
An important lesson of the Sofaer case can be found in the court's observation that Sofaer did not (as any lawyer could have) "solicit the views of his or her former agency concerning the proposed private legal undertaking" or "consult with ethics advisers in his or her law firm . . . or with the Legal Ethics Committee of the Bar." 109

1. Diligence

A lawyer shall act with reasonable diligence and promptness in representing a client.110

Do the time-sensitive exigencies of national security law "matter" in ethical decision making? Perhaps the real issue for the national security law practitioner is to determine what is "reasonable" diligence under the circumstances of a national security crisis. Unfortunately, no database or treatise defines "reasonable" in the myriad of situations that national security law practitioners face. In fact, many issues may be ones of first impression, so there may well be a lack of historical precedent to rely upon.

Time pressure can be very real. In a statement submitted in connection with David Margolis' examination of the OPR conclusion that the two OLC attorneys, John Yoo and Jay Bybee, violated ethical rules in the opinions about enhanced interrogation techniques that many consider torture, Professor Jack Goldsmith contends:

OPR is not looking at the OLC opinions with the same time constraints as the lawyers who wrote the opinions; instead OPR has taken nearly five years and still has not rendered a judgment. The OLC layers did not have this luxury. Perhaps more important, OPR is looking at the OLC opinions not in the context of the threat and danger in which they were written, but rather in what former Deputy Attorney General James Comey once described as "the perfect, and brutally unfair, vision of hindsight." 111


110. MODEL RULES, supra note 16, R. 1.3.

111. Memorandum from David Margolis, supra note 11.
In its guidance on ethical decision making, the Department of Defense Joint Ethics Regulation advises: "The stress from the problem urges speedy solutions. However, hasty decisions usually create problems of their own. Take the time to gather all necessary information. Ask questions, demand proof when appropriate, check your assumptions."\textsuperscript{112}

Taking "the time to gather all necessary information" may be fine as hortatory and aspirational statement, but is often impractical given the velocity of many if not most national security issues. Hard decisions often must be made on less than ideal information. Judge James Baker, a former National Security Council member, observes that today’s national security attorneys may not have much time for deliberation.\textsuperscript{113} "For a variety of reasons," he says, "relating to the nature and multiplicity of transnational and state threats, combined with the devastating potential of WMD, questions of whether to resort to force and the methods and means of force will pop-up and require immediate decision."\textsuperscript{114}

Of course, when time to study an issue is available, it can make a real difference. In a Human Rights Watch study about operations in Afghanistan, it was found that civilian casualties "rarely occur during planned airstrikes on suspected Taliban targets" but rather "almost always occurred during the fluid, rapid-response strikes, often carried out in support of ground troops."\textsuperscript{115}

The "time crunch" of many national security issues highlights the importance of advance preparation. The ability to make quick decisions much depends not just upon an in-depth understanding of the law, but also upon thorough familiarity with the context in which it must be applied. As explained with relation to the ethical rule about competence, the ability to be diligent in a national security law practice requires the attorneys involved to make a study of the means and methods of national security operations.

As discussed elsewhere in this Article, diligence in the national security law context may impose a responsibility to conduct a careful after-action examination to ensure that decisions made in—literally—the heat of battle were the right ones.


\textsuperscript{114} Id.

g. Confidentiality

A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation... A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:... to prevent reasonably certain death or substantial bodily harm... or (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another... 116

The case of former Navy Lieutenant Matthew Diaz is instructive with respect to the complications of confidentiality in the national security context. Diaz was a Navy Judge Advocate assigned to Guantánamo, Cuba, not as part of the prosecution or defense teams involved in military commissions' cases, but rather as part of the installation support legal office.117 In that capacity he served as the point of contact at Guantánamo for requests from Barbara Olshansky, an attorney working for the Center for Constitutional Rights ("CCR") in New York City, who was seeking names and information regarding detainees.118

116. MODEL RULES, supra note 16, R. 1.6. The full rule reads as follows:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;
(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;
(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;
(4) to secure legal advice about the lawyer's compliance with these Rules;
(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or
(6) to comply with other law or a court order.


118. See id.
After a decision was made to not provide the information to Olshansky, Diaz concluded that the "government was 'stonewalling' over the release of the names." Consequently, Diaz printed off a list of 550 detainees, and sent it anonymously in a Valentine's card to Olshansky. Suspecting the list was classified, Olshansky contacted an attorney and eventually turned the list over to government authorities who launched an investigation, which nabbed Diaz.

According to his defense counsel, Diaz believed it was his "obligation as a lawyer and an American to abide by the Constitution when he felt the government did not." However, the military judge in the case concluded "that none of the evidence proffered by Appellant supported his argument that he was required to release classified information based on his duties as a commissioned officer, his ethical obligations as a judge advocate, or his ethical obligations as a licensed attorney." Although his attorney admitted that Diaz was "stupid, imprudent and sneaky, if you want, about the way he sent it off," he nevertheless insisted Diaz "didn't mean to harm his country." Still, Diaz was convicted and sentenced to six months confinement and dismissal from the Navy.

The Court of Appeals for the Armed Forces affirmed the conviction and sentence. A footnote in the court's opinion is telling. In it, the court described the process available to Navy lawyers who believe they are confronting an ethical conundrum. Referring to Navy instruction on professional responsibility, the court points out that it "recommends four specific steps a covered attorney might take, including 'refer[ring] the matter to, or seek[ing] guidance from, higher authority in the chain of command.'" Of course, Diaz had made no attempt to resolve his concerns in this way.

The lesson here may be that as important as it is for national security practitioners to be self-governing, it does not mean that "self-help" in the area of ethics is necessarily appropriate. Reaching out to experts as
provided by ethics rules is especially important in the complex arena of national security law. Here the facts did not support Diaz’s belief (however earnestly held) that he was in an ethical conflict, which strongly suggests that consultation with superiors and others qualified to offer advice might have avoided the career implosion he underwent.

h. Client Relations

A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.\(^{129}\)

129. Model Rules, supra note 16, R. 1.6. The full rule reads as follows:

(a) A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.

(b) If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action, intends to act or refuses to act in a matter related to the representation that is a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, then the lawyer shall proceed as is reasonably necessary in the best interest of the organization. Unless the lawyer reasonably believes that it is not necessary in the best interest of the organization to do so, the lawyer shall refer the matter to higher authority in the organization, including, if warranted by the circumstances, to the highest authority that can act on behalf of the organization as determined by applicable law.

(c) Except as provided in paragraph (d), if

(1) despite the lawyer’s efforts in accordance with paragraph (b) the highest authority that can act on behalf of the organization insists upon or fails to address in a timely and appropriate manner an action, or a refusal to act, that is clearly a violation of law, and

(2) the lawyer reasonably believes that the violation is reasonably certain to result in substantial injury to the organization, then the lawyer may reveal information relating to the representation whether or not Rule 1.6 permits such disclosure, but only if and to the extent the lawyer reasonably believes necessary to prevent substantial injury to the organization.

(d) Paragraph (c) shall not apply with respect to information relating to a lawyer’s representation of an organization to investigate an alleged violation of law, or to defend the organization or an officer, employee or other constituent associated with the organization against a claim arising out of an alleged violation of law.

(e) A lawyer who reasonably believes that he or she has been discharged because of the lawyer’s actions taken pursuant to paragraphs (b) or (c), or who withdraws under circumstances that require or permit the lawyer to take action under either of those paragraphs, shall proceed as the lawyer reasonably believes necessary to assure that the organization’s highest authority is informed of the lawyer’s discharge or withdrawal.

(f) In dealing with an organization’s directors, officers, employees, members, shareholders or other constituents, a lawyer shall explain the identity of the client when the lawyer knows or reasonably should know that the organization’s interests are adverse to those of the constituents with whom the lawyer is dealing.

(g) A lawyer representing an organization may also represent any of its directors, officers, employees, members, shareholders or other constituents, subject to the provisions of Rule 1.7. If the organization’s consent to the dual representation is required by Rule 1.7, the consent shall be given by an appropriate official of the organization other than the individual who is to be represented, or by the shareholders.
In a national security law practice, the "who is the client" query can be a complicated question. Harold Koh, the legal advisor to the State Department, lists a number of *individuals* among those who he characterizes as his "extraordinary" clients.⁷ These include, for example, Secretary of State Hillary Clinton, and the President.⁸ Such individual representation is, however, the exception, not the rule for most governmental national security law practitioners.

The District of Columbia Rules of Professional Responsibility, for example, provide that the "client of the government lawyer is the agency that employs the lawyer unless expressly provided to the contrary by appropriate law, regulation, or order." Some agencies make this explicit.

---


131. See id.

132. *D.C. RULES OF PROF'L CONDUCT R. 1.6(k) (2006), available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/rules_of_professional_conduct/amended_rules/rule _one/rule01_06.cfm. The commentary to the rule provides as follows:

**Government Lawyers**

[36] Subparagraph (e)(2) was revised, and paragraph (k) was added, to address the unique circumstances raised by attorney-client relationships within the government.

[37] Subparagraph (e)(2)(A) applies to both private and government attorney-client relationships. Subparagraph (e)(2)(B) applies to government lawyers only. It is designed to permit disclosures that are not required by law or court order under Rule 1.6(e)(2)(A), but which the government authorizes its attorneys to make in connection with their professional services to the government. Such disclosures may be authorized or required by statute, executive order, or regulation, depending on the constitutional or statutory powers of the authorizing entity. If so authorized or required, subparagraph (e)(2)(B) governs.

[38] The term "agency" in paragraph (j) includes, *inter alia*, executive and independent departments and agencies, special commissions, committees of the legislature, agencies of the legislative branch such as the Government Accountability Office, and the courts to the extent that they employ lawyers (e.g., staff counsel) to counsel them. The employing agency has been designated the client under this rule to provide a commonly understood and easily determinable point for identifying the government client.

[39] Government lawyers may also be assigned to provide an individual with counsel or representation in circumstances that make clear that an obligation of confidentiality runs directly to that individual and that subparagraph (e)(2)(A), not (e)(2)(B), applies. It is, of course, acceptable in this circumstance for a government lawyer to make disclosures about the individual representation to supervisors or others within the employing governmental agency so long as such disclosures are made in the context of, and consistent with, the agency's representation program. See, e.g., 28 C.F.R. § 50.15 and § 50.16. The relevant circumstances, including the agreement to represent the individual, may also indicate whether the individual client to whom the government lawyer is assigned will be deemed to have granted or denied informed consent to disclosures to the lawyer's employing agency. Examples of such representation include representation by a public defender, a government lawyer representing a defendant sued for damages arising out of the performance of the
In the U.S. Air Force, the Rules of Professional Conduct state that "[e]xcept when authorized to represent an individual client or the government of the United States, an Air Force judge advocate or other Air Force lawyer represents the Department of the Air Force acting through its authorized officials." The explanatory notes point out that when "an Air Force official, member, or employee, acting within the scope of his or her official duties, communicates with an Air Force lawyer, the communication is confidential [and] . . . . [u]nder these circumstances, the official, member or employee is, in essence, the Air Force." As both military officers and legal professionals, attorneys in the armed forces face practical challenges. It is easy in the military for a commander to assume that the uniformed lawyer assigned to his unit is also "his" personal counsel, notwithstanding circumstances where the Air Force's interests conflict with those of individuals, including commanders. Thus, it is especially important that this be made clear before there is any misunderstanding about client confidences.

The "who is the client?" question can become even more complicated for military lawyers and others assigned to commands composed of international partners. Even though, for example, an attorney may be assigned as a legal advisor to a coalition operation, the client will remain the attorney's sponsoring organization (e.g., the U.S. Air Force).

There is a practical issue as well—few lawyers would be competent to advise other national contingents on their national responsibilities, not to mention their international responsibilities under treaty law where the interpretation may be subject to particular reservations and other qualifications by a specific coalition partner. It is imperative, then, that a lawyer so assigned make clear the limits of the legal assistance he or she can provide.

Like the Navy, the Air Force has a process by which military attorneys can seek ethical and other guidance from senior lawyers,

defendant's government employment, and a military lawyer representing a court-martial defendant.


134. Id.

135. See, e.g., Id., R. 1.13(d) ("In dealing with Air Force officials, members, employees, or other persons associated with the Air Force, a lawyer shall explain that the Air Force is the lawyer's client when it is apparent that the Air Force's interests are adverse to those of the officials, members, or employees with whom the lawyer is dealing.").

136. See Díaz, 69 M.J. at 136 n.11.
especially when confronted with situations where the attorney believes that an Air Force official "is acting, intends to act, or refuses to act in an official matter in a way that is either a violation of the person's legal obligations to the Air Force or a violation of law which reasonably might be imputed to the Air Force."\textsuperscript{137}

This access to advice and guidance from senior attorneys is protected by law. For example, the Uniform Code of Military Justice specifically states that military legal officers are "entitled to communicate directly with the staff judge advocate or legal officer of a superior or subordinate command, or with the Judge Advocate General."\textsuperscript{138} The ability to circumvent, if necessary, the normal chain of command is no small prerogative given that the "the Armed Services comprise a hierarchical society, which is based on military rank."\textsuperscript{139}

The law also helps assure the organization gets candid, apolitical legal advice from military lawyers. In fact, the law prohibits any interference from any "officer or employee of the Department of Defense" with respect to the rendering of "independent legal advice."\textsuperscript{140} Furthermore, in order to reinforce the independence of the provision of legal advice from uniformed attorneys, the law also designates the Judge Advocate General, as opposed to any non-legal officer, as responsible for directing "the officers of the Air Force designated as judge advocates in the performance of their duties."\textsuperscript{141} All of these statutory provisions help ensure that a military lawyer can carry out his or her ethical responsibilities to the organizational client without running afoul of the duties and responsibilities of a commissioned officer. They are also invaluable in ensuring the delivery of independent and candid advice, as discussed below.

\textsuperscript{137} AIR FORCE RULES, supra note 133, R. 1.13(b).
\textsuperscript{138} 10 U.S.C § 806 (2011).
\textsuperscript{139} U.S. v. Means, 10 M.J. 162, 165 (C.M.A. 1981).
\textsuperscript{140} 10 U.S.C § 8037(f) provides:

(1) No officer or employee of the Department of Defense may interfere with—
(1) the ability of the Judge Advocate General to give independent legal advice to the Secretary of the Air Force or the Chief of Staff of the Air Force; or
(2) the ability of officers of the Air Force who are designated as judge advocates who are assigned or attached to, or performing duty with, military units to give independent legal advice to commanders.

\textsuperscript{141} 10 U.S.C § 8037(f) (2011).
i. Lawyer as Advisor

In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client’s situation.142

This section is one of the most important parts of the Model Rules for the national security law practitioner. The very nature of many national security issues is such that their proper resolution can only be had when a range of factors—such as those listed in the rule—are brought to bear on the client’s situation. Yet there are some national security lawyers who perceive their role rather narrowly. Judge Alberto Gonzales, the former Attorney General who has been soundly critiqued for his part in the rendering of suspect advice on coercive interrogation techniques, said in an interview for Esquire magazine, “Putting my lawyer hat aside, the notion that we’d have to get legalistic about torture, yeah, can be offensive to me. It’s inconsistent with American values. But as a lawyer—as a lawyer—you have to try to put meaning to the words passed by Congress.”143

Actually, if the law is truly inconsistent with “American values” then the law itself is suspect, and the national security lawyer needs to make this clear to the client. Perspective matters. In a 2006 essay entitled “Cooler Heads: The Difference between the President’s Lawyers and the Military’s,” Professor Richard Schragger illustrated this importance of perspective. In discussing the dispute at that time between military lawyers (who eschewed coercive interrogation techniques and other actions designed to eviscerate the Geneva Conventions and certain aspects of international and domestic law) and the then-Administration’s civilian attorneys who advocated just such approaches, Schragger concluded:

[M]ilitary lawyers understand that when you ask human beings to kill other human beings, rules of decency are required. War does not erase the line between legal and illegal killings, legal and illegal acts—war accentuates it. Establishing and policing that line becomes even more important when your client is the one likely to cross it.

Civilian lawyers may not appreciate this. Civilian lawyers are educated and socialized into a legal culture that takes the rule of law for granted. The stability of our legal system allows us to do what we do best: seek ways for our clients to avoid legal mishap. The law is something we need to strategize around because it often functions to limit our clients’ options, not serve them.\textsuperscript{144}

It is just these kinds of subtleties that can be vitally important in national security matters, and is a clear reason why the broader scope of advice a lawyer can provide is so important. Moreover, it is vital for a national security practitioner not to underestimate the extreme pressure under which some clients must operate. Consider the observation of a former senior military commander:

When I go to my lawyers, I don’t ask, “okay, tell me how I can’t do this.” I go to my lawyers and say, “How can I do what I need to do and not go to jail? How can I do it legally? . . . The legal advisor has to understand that his job is to find a way through the interpretations and legal precedence for the things we have to do, so I can protect my people going out in harms’ way.”\textsuperscript{145}

Sensitivity to the often life-and-death nature of national security issues cannot be overemphasized, and it is one reason why the national security law practitioner needs to be prepared to bring to bear every relevant consideration to the decision-making process, legal and otherwise. At the same time, however, the practitioner needs to keep in mind that there must be a clear distinction between legal advice, and advice that incorporates considerations that fall short of a legal mandate. However, the lawyer’s recommendation need not yield to simply giving “meaning to the words passed by Congress.”\textsuperscript{146}

National security clients need more from their lawyers than mere rote recitations of the meanings of statutes. Senator Lindsey Graham said in a 2004 interview that the “military lawyer [JAG] is really the conscience of the military.”\textsuperscript{147} Similarly, Harold Koh said that his State Department

\textsuperscript{144} Richard C. Schragger, Cooler Heads: The difference between the president’s lawyers and the military’s, SLATE (Sept. 20, 2006, 5:10 PM), http://www.slate.com/id/2150050/?nav/navoa


\textsuperscript{146} See Richardson, supra note 143.

\textsuperscript{147} Interview with Lindsey Graham, FRONTLINE (Oct. 26, 2004), http://www.pbs.org/wgbh/pages/frontline/shows/pentagon/interviews/graham.html.
attorneys serve as the "conscience for the U.S. Government with regard to international law."\textsuperscript{148}

Koh goes on to explain that "one of the most important roles of the Legal Adviser is to advise the Secretary when a policy option being proposed is 'lawful but awful.'"\textsuperscript{149} He then quotes one of his predecessors, Herman Pfleger, for the proposition that, "You should never say no to your client when the law and your conscience say yes; but you should never, ever say yes when your law and conscience say no."\textsuperscript{150} This is advice the national security practitioner might find useful to keep in mind if confronted with a situation that is, as Judge Gonzales puts it, "inconsistent with American values."\textsuperscript{151}

\textbf{j. Conduct Before a Tribunal}

A lawyer shall not knowingly: (1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer; (2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or (3) offer evidence that the lawyer knows to be false . . . .\textsuperscript{152}

As we have already seen, the importance of candor for the national security practitioners is critical as so many of the cases involve either matters that are properly classified, or issues in which the courts depend upon the integrity of the government representations. Unfortunate'y, history

\textsuperscript{148} Koh, supra note 130.
\textsuperscript{149} Id.
\textsuperscript{150} Id.
\textsuperscript{151} Richardson, supra note 143.
\textsuperscript{152} MODEL RULES, supra note 16, R. 3.3. The full paragraph (a) reads as follows:

(a) A lawyer shall not knowingly:
(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
(2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or
(3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.

Id.
shows that reliance is not always justified. Classic examples are the World War II Japanese internment cases, *Korematsu v. U.S.*\(^{153}\) and *Hirabayashi v. U.S.*\(^{154}\).

After the Japanese attack on Pearl Harbor in 1941, war hysteria eventually turned on thousands of Japanese-Americans living on the West Coast.\(^{155}\) Because they were suspected of being potential “fifth columnists” or spies, President Roosevelt issued an executive order authorizing military authorities to remove Japanese-Americans from areas near the coast.\(^{156}\) Eventually, 100,000 were removed and sent to internment camps.\(^{157}\) The Japanese Internment Cases challenged these actions, but in both instances the government’s authority was upheld.\(^{158}\)

In 2011, however, Neal Katyal, the then Acting Solicitor General of the United States, made a series of disclosures that reflect poorly on the ethics of his World War II predecessor, Charles Fahy.\(^{159}\) Katyal reports that a critical intelligence document—the Ringle Report—“found that only a small percentage of Japanese Americans posed a potential security threat, and that the most dangerous were already known or in custody.”\(^{160}\) Even though the Solicitor General knew of this very significant information, he withheld it from the Supreme Court.\(^{161}\)

Instead, the Solicitor General “argued that it was impossible to segregate loyal Japanese Americans from disloyal ones.”\(^{162}\) He also failed to tell the Court that allegations “that Japanese Americans were using radio transmitters to communicate with enemy submarines off the West Coast, had been discredited by the FBI and FCC.”\(^{163}\) According to Katyal, “to make matters worse, [he then] relied on gross generalizations about Japanese Americans, such as that they were disloyal and motivated by ‘racial solidarity.’”\(^{164}\)

---

154. 320 U.S. 81 (1943).
155. See generally id. at 113-14.
159. See Russo, supra note 157.
160. Id.
161. See id.
162. Id.
163. Id.
164. See Russo, supra note 157.
This ethically horrific behavior by a lawyer holding such an important public office is hard to fathom, but does represent how a wartime mania can warp the thinking of the very people whom democracies depend upon to be paragons of composure and rational behavior. Can we dismiss these cases as anomalies from more than half a century ago? Consider the case of Ashcroft v. al-Kidd.165

Al-Kidd involved a Kansas-born, former University of Idaho football player named Lavni T. Kidd who converted to Islam while in college and changed his name to Abdullah al-Kidd.166 After 9/11, al-Kidd was questioned by authorities about an acquaintance, a Saudi graduate student named Sami Omar al-Hussayen, who was suspected of using his computer skills to aid terrorists.167 Although he cooperated with the FBI when asked about al-Hussayen, al-Kidd was arrested on a “material witness” warrant in 2003 as he boarded a plane to Saudi Arabia to take a course of study in Islam.168 The affidavits that the FBI used to obtain the warrant proved to be wildly inaccurate.169

Al-Kidd was kept in jail for sixteen days and on supervised release until al-Hussayen’s trial concluded fourteen months later.170 According to the American Civil Liberties Union, while in federal custody, al-Kidd was “kept under extremely harsh conditions,” including being “kept awake for hours on end, with a bright light shining in his cell 24/7.”171 In addition, whenever he left his cell he was “shackled at the wrists, ankles, and waist” and at “one point, he was left naked for hours in plain view of other clothed prisoners and guards.”172 What is more, when released from jail, he was still “kept under restrictive conditions for months that forced him to abandon an educational scholarship and led to the breakdown of his marriage and career.”173

Importantly, al-Kidd was not the only Muslim-American treated this way. According to the Associated Press, al-Kidd was one of “about 70 men, almost all Muslims, who were arrested and held in the months and

166. See al-Kidd v. Ashcroft, 580 F.3d 949, 952 (9th Cir. 2009).
167. See id.
169. See al-Kidd, 580 F.3d at 953.
170. See id.
172. Id.
173. Id.
years after Sept. 11” under the material witness statute. At the time, Attorney General John Ashcroft, like other officials, bragged that “aggressive detention of lawbreakers and material witnesses is vital to preventing, disrupting or delaying new attacks.” Like many others, al-Kidd was never called as a witness or charged with any crime (and al-Hussayen was tried but not convicted).

After his release al-Kidd sued Ashcroft claiming, in essence, that the former U.S. Attorney General had had his subordinates use the Material Witness Statute as a pretext to detain terrorist suspects preventively, that is, persons suspected of terrorism but for whom evidence was lacking for an arrest and criminal charge. After extended litigation, the Supreme Court held that Ashcroft was entitled to qualified immunity because “at the time of [the detainee’s] arrest . . . not a single judicial opinion had held that pretext could render an objectively reasonable arrest pursuant to a material-witness warrant unconstitutional.”

Although she concurred in the outcome, Justice Ginsburg (with Justices Breyer and Sotomayor) nevertheless found the Court’s assumption of the existence of a validly obtained material witness warrant to be “puzzling.” She questioned whether an affidavit supporting a material witness warrant is valid where the affiant fails to tell the issuing magistrate that there is no intent to call the subject of the warrant as a witness in any trial. She also questioned the validity of the warrant where the affidavit “[did] not disclose that al-Kidd had cooperated with FBI agents each of the several times they had asked to interview him.” In addition, she said:

> The Magistrate Judge was not told that al-Kidd’s parents, wife, and children were all citizens and residents of the United States. In addition, the affidavit misrepresented that al-Kidd was about to take a one-way flight to Saudi Arabia, with a first-class ticket costing

---

175. Id.
177. See al-Kidd, 580 F.3d at 955–56.
178. Al-Kidd, 131 S. Ct. at 2074.
179. See id. at 2087 (Ginsburg, J., concurring).
180. See id.
181. See id.
approximately $5,000; in fact, al-Kidd had a round-trip, coach-class ticket that cost $1,700.  

With this cacophony of misstatements and omissions in the material used to justify the warrant, the case went back to the district court, where a federal magistrate was appointed to do a report and recommendation on cross-motions for summary judgment involving two individual defendants (the FBI agents), and a report and recommendation on cross-motions for summary judgment involving the United States. Both of these reports generally favored al-Kidd, and may lead to his eventual compensation for what he underwent.

What is, to use Justice Ginsburg’s word, “puzzling” is the role of the lawyers in al-Kidd. Just because they may enjoy qualified immunity does not explain how or why the affidavit misinformation that Justice Ginsburg cited in her opinion failed to free al-Kidd from the restrictions earlier. Even if the attorneys involved did not manufacture the misinformation, at some point during al-Kidd’s ordeal someone from the government should have stepped forward to correct the record. It would seem that, at a minimum, a better exercise of due diligence in the case of an individual being detained without charges would be the ethically proper approach.

Moreover, despite the Court’s finding that there were no cases finding a pretextual use of a material witness warrant unconstitutional, it would also seem ironic that more had not been learned from the Japanese internment cases. They ought to stand for the proposition that preventive detention by any other name is still preventive detention, and that is something Congress has yet to authorize in terrorism cases for American citizens residing in the United States. The national security practitioner, while remaining open to innovative interpretations of the law, nonetheless must be extremely wary of proposals which have atrocious parallels in history.

---

182. See id. at 2088.
k. Pro Bono

Every lawyer has a professional responsibility to provide legal services to those unable to pay.186

One of the most interesting impacts on the legal profession of the post-9/11 era is the proliferation of pro bono legal support for the suspected terrorists detained at Guantánamo. Professor Jack Goldsmith of Harvard points out that after the Supreme Court’s landmark 2004 decision in Rasul v. Bush187 established that the detainees were entitled to challenge their detention in the courts, “pro bono offers from hundreds of attorneys, including many from America’s most elite law firms[,]” came to the detainees.188 According to Goldsmith, these “lawyers—who came to be known as ‘the GTMO Bar’—quickly flooded federal courts with habeas corpus petitions from detainees seeking release.”189

186. MODEL RULES, supra note 16, R. 6.1. The full rule reads as follows:

Every lawyer has a professional responsibility to provide legal services to those unable to pay. A lawyer should aspire to render at least (30) hours of pro bono publico legal services per year. In fulfilling this responsibility, the lawyer should:

(a) provide a substantial majority of the (30) hours of legal services without fee or expectation of fee to:

(1) persons of limited means or
(2) charitable, religious, civic, community, governmental and educational organizations in matters that are designed primarily to address the needs of persons of limited means; and

(b) provide any additional services through:

(1) delivery of legal services at no fee or substantially reduced fee to individuals, groups or organizations seeking to secure or protect civil rights, civil liberties or public rights, or charitable, religious, civic, community, governmental and educational organizations in matters in furtherance of their organizational purposes, where the payment of standard legal fees would significantly deplete the organization’s economic resources or would be otherwise inappropriate;
(2) delivery of legal services at a substantially reduced fee to persons of limited means; or
(3) participation in activities for improving the law, the legal system or the legal profession.

In addition, a lawyer should voluntarily contribute financial support to organizations that provide legal services to persons of limited means.

Id. 187. 542 U.S. 466 (2004).
189. Id. For a discussion of habeas corpus actions, see generally Habeas Corpus, LEGAL INFORMATION INSTITUTE (Aug. 19, 2010, 5:17 PM), http://www.law.cornell.edu/wex/habeas_corpus.
Other experts recently noted that since “2002, over 900 attorneys have joined the network sponsored by [Center for Constitutional Rights] filing individual habeas petitions for approximately 430 detainees.”190 According to these analysts, after several Supreme Court cases legitimated habeas litigation:

[Large firms sought out habeas clients—the legal market favored firm representation of detainees. In fact, representation of Guantánamo detainees became part of law firms’ recruitment efforts for new associates. Yet the cases did not only appeal to lawyers new to the practice. Detainee representation was high-profile legal work, and the firms staked these matters with senior partners, signaling to attorneys within the firm, as well as to clients, the value the firm placed on the work.191]

A media report similarly reflected the popularity of detainee representation. As one lawyer involved in the process put it:

“I had always worried that we would get some input from clients that was less than supportive,” [the defense counsel] said. “But we must have gotten 10 e-mails, phone calls, personal contacts from Fortune 500 companies that said the opposite. One big client said, ‘That makes me want to send you more work—not less.’”192

It was perhaps frustration over the enormous resources the civilian bar provided the terrorist suspects that led a former Deputy Assistant Secretary of Defense for Detainee Affairs, Cully Stimson, to make some profoundly ill-considered remarks. In a 2007 interview, he expressed dismay “that lawyers at many of the nation’s top firms were representing prisoners at Guantánamo Bay, Cuba, and that the firms’ corporate clients should consider ending their business ties.”193

Predictably, there was an explosion of criticism, with numerous commentators rebuking Stimson for attacking the honorable practice of providing vigorous, pro bono representation to even the most reviled accused. The obviously upset editors of the Washington Post wrote that the

191. Id at 650 (emphasis added).
detainee lawyers were "upholding the highest ethical traditions of the bar by taking on the most unpopular of defendants." 194 Though not offering a defense for Stimson's remarks, Harvard law professor Charles Fried speculated that perhaps Stimson was "annoyed that his overstretched staff lawyers are opposed by highly trained and motivated elite lawyers working in fancy offices with art work in the corridors and free lunch laid on in sumptuous cafeterias." 195 Regardless, Stimson apologized and promptly resigned in an effort to quiet the furor. 196

Similar criticism arose in 2010 amid questions about the Justice Department's hiring of a number of lawyers who had previously represented Guantanamo detainees. In an open letter, a group of "attorneys, former officials, and policy specialists who have worked on detention issues" admirably stated the case:

The American tradition of zealous representation of unpopular clients is at least as old as John Adams's representation of the British soldiers charged in the Boston massacre. People come to serve in the Justice Department with a diverse array of prior private clients; that is one of the department's strengths . . . . To suggest that the Justice Department should not employ talented lawyers who have advocated on behalf of detainees maligns the patriotism of people who have taken honorable positions on contested questions and demands a uniformity of background and view in government service from which no administration would benefit. 197

Yet even as one salutes the outpouring of pro bono support for the terrorist detainees, support that no doubt can be traced to finest traditions of the Bar to provide quality representation to all accused, concern must be expressed by the paradox that foreign terrorists may be—proportionately—greater beneficiaries of the legal profession's beneficence than are needy U.S. citizens not accused of national security crimes.

This paradox is suggested by Attorney General Eric Holder's speech to the ABA in February 2012. In it he lamented the "crisis" with respect to indigents' access to legal talent:

search.html.
Across the country, public defender offices and other indigent defense providers are underfunded and understaffed. Too often, when legal representation is available to the poor, it's rendered less effective by insufficient resources, overwhelming caseloads, and inadequate oversight.

As a result, too many defendants are left to languish in jail for weeks, or even months, before counsel is appointed. Too many children and adults enter the criminal justice system with nowhere to turn for guidance—and little understanding of their rights, the charges against them, or the potential sentences—and collateral consequences—that they face. Some are even encouraged to waive their right to counsel altogether.\footnote{198}

It is not without irony then, that the legal profession, notwithstanding its outpouring of very healthy support for foreign terrorist detainees, nevertheless finds itself facing inadequate representation for needy Americans.\footnote{199} This is plainly an appropriate subject not only for national security practitioners but for the entire bar. Nevertheless, the real test of the national security bar’s ethics may come if (when?) there is another horrific event, and doing the right thing by defending accused terrorists is not as popular as it may be today. It is in times of crisis that the ethics of the legal profession are most tested, and practitioners need to steel themselves for those moments—which are sure to come to pass.

III. CONCLUDING OBSERVATION: THE INDISPENSABILITY OF MORAL COURAGE

Although this Article has sought to illustrate some of the ethical challenges national security law practitioners face, it would be a mistake to assume that national security practitioners are somehow more prone to ethical failings than others in the legal profession. Nothing could be further from the facts.

Professor H. Jefferson Powell, who until May 2012 served as the deputy assistant attorney general in the OLC at the Department of Justice, reflected upon his work with lawyers in a range of government agencies and commented that what struck him was “how dedicated the vast majority of those people are to doing responsible legal work, in good faith and for the


\footnote{199: Compare id. with Shukovsky, supra note 192.}
highest of motives—pro bono publico, for the public good. He added that what impressed him “about the vast majority of the lawyers with whom [he] dealt is their conscientious commitment to the law and to providing responsible legal advice.”

Powell also believed the “particular contribution of government lawyers” is to “enable the government to function and to pursue the policies that the policymakers prefer but to do so within the law [and] to tell the policymakers when necessary that a particular goal or policy cannot be pursued lawfully.” In the national security context, this can be particularly difficult because the stakes are so high, time is so short, and the consequences of the proverbial path not taken are difficult to ascertain or predict.

Telling policymakers and other clients what they need to hear versus what they may want to hear requires courage; indeed, few legal disciplines require the practitioners to exhibit as much courage as does a national security law practice. Unlike most national security activities, the kind of courage required is not, however, the physical type, but moral courage. This can be hard to muster for anyone, even in the armed forces. British historian Max Hastings points out that “physical bravery is found [in the military] more often than the spiritual variety.” “Moral courage,” he says, “is rare.” Yet it is especially important for those in the legal profession to demonstrate it. There is no doubt that in national security matters especially, there are times when legal advice is unwelcome, but that is when moral courage is most needed. General Short admonishes that in combat situations:

[D]o not be afraid to tell [the commander] what he really does not want to hear—that he has put together this exquisite plan, but his targets indeed are not valid ones or his targets may in fact violate the law of armed conflict . . . . It will take enormous courage to do

201. Id.
202. Id.
203. In a 1990 case called U.S. v. Stidman, the Air Force Court of Criminal Appeals observed:

[T]here are two kinds of courage involved in the profession of arms and the profession of law. On the one hand, many are called upon for physical courage. On the other hand, judges are called upon from time to time for moral courage—the courage to subordinate a personal philosophy of the law or private distress . . . . to decide an issue logically and dispassionately.

205. Id.
that in particular circumstances because you're always going to be junior to your boss . . . . But you have got to be able to do that.\textsuperscript{206}

Judge James E. Baker of the Court of Appeals for the Armed Forces argues in his book \textit{In the Common Defense} that the law depends upon the "moral courage of lawyers who raise tough questions, who dare to argue both sides of every issue, who insist on being heard at the highest levels of decision-making, and who ultimately call the legal questions as they believe the Constitution dictates . . . .\textsuperscript{207}

Judge Baker is, of course, exactly right. No set of rules can substitute for the character of individuals who are ready to do the right thing, regardless of the personal consequences. Only those prepared to make whatever sacrifice is necessary to ensure that the nation conducts its national security affairs in a lawful—and authentically ethical—manner are truly worthy of the sobriquet of a national security law practitioner.

\textsuperscript{206} Operation Allied Force, supra note 91.
\textsuperscript{207} JAMES E. BAKER, \textit{IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS ISSUES} 325 (2007).