CONFERENCE MATERIAL

DAY ONE

SPONSORED BY:

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

CENTER FOR NATIONAL SECURITY LAW
UNIVERSITY OF VIRGINIA SCHOOL OF LAW

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

CENTER ON NATIONAL SECURITY AND THE LAW
GEORGETOWN LAW

OCTOBER 31—NOVEMBER 1, 2013

RITZ-CARLTON HOTEL
SALONS I AND II
1150 22ND STREET, NW
WASHINGTON, DC
## Panel I
### Executive Updates on Developments in National Security Law

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy, Technology and National Security: An Overview of Intelligence Collection - Robert S. Litt</td>
<td>1</td>
</tr>
<tr>
<td>Letters to the Honorable Charles E. Grassley - Honorable Reggie B. Walton</td>
<td>19</td>
</tr>
<tr>
<td>Rules of Procedure (Effective November 1, 2013) - United States Foreign Intelligence Surveillance Court</td>
<td>33</td>
</tr>
<tr>
<td>Letter to the Honorable Dianne Feinstein - Honorable Reggie B. Walton</td>
<td>51</td>
</tr>
<tr>
<td>Joint Statements before the Senate Committee on the Judiciary (October 2, 2013) - James R. Clapper and General Keith B. Alexander</td>
<td>55</td>
</tr>
<tr>
<td>Joint Statements before the Senate Select Committee on Intelligence (September 26, 2013) - James R. Clapper, General Keith B. Alexander and James M. Cole</td>
<td>67</td>
</tr>
<tr>
<td>Why Drones Work: The Case for Washington’s Weapon of Choice - Daniel L. Byman</td>
<td>79</td>
</tr>
<tr>
<td>Why Drones Fail: When Tactics Drive Strategy - Audrey Kurth Cronin</td>
<td>87</td>
</tr>
<tr>
<td>Projecting Force in the 21st Century - Legitimacy and the Rule of Law - Jeff Mustin and Harvey Rishikof</td>
<td>93</td>
</tr>
<tr>
<td>Demystifying the Title 10 - Title 50 Debate: Distinguishing Military Operations, Intelligence Activities &amp; Covert Action - Andru E. Wall</td>
<td>111</td>
</tr>
<tr>
<td>Clapper v. Amnesty International USA - Supreme Court of the United States</td>
<td>169</td>
</tr>
</tbody>
</table>

## Panel II
### Legislative Updates on Developments in National Security Law

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Fears Slowed Aid to Syrian Rebels - Adam Entous</td>
<td>237</td>
</tr>
<tr>
<td>Afghan War’s Approaching End Throws Legal Status of Guantanamo Detainees into Doubt - Karen DeYoung</td>
<td>251</td>
</tr>
<tr>
<td>The Future of our Fight against Terrorism - Remarks of President Barack Obama (NDU, May 23, 2013)</td>
<td>255</td>
</tr>
<tr>
<td>Rules of Procedure for the Senate Select Committee on Intelligence, Appx. A (Amended March 1, 2007)</td>
<td>269</td>
</tr>
</tbody>
</table>

## Keynote Discussion
### Critical National Security Cases to Watch

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. v. Bond - United States Court of Appeals, Third Circuit</td>
<td>279</td>
</tr>
<tr>
<td>Al-Aulaqi v. Panetta - United States District Court for the District of Columbia</td>
<td>301</td>
</tr>
<tr>
<td>United States of America v. Al Bahlul - United States Court of Military Commission Review</td>
<td>319</td>
</tr>
<tr>
<td>ACLU v. James R. Clapper - United States District Court Southern District of New York</td>
<td>459</td>
</tr>
<tr>
<td>In re Electronic Privacy Information Center - Supreme Court of the United States</td>
<td>471</td>
</tr>
</tbody>
</table>
## Panel III

**Do We Need a New AUMF?**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jihadist Terrorism: A Threat Assessment - Bipartisan Policy Center</td>
<td>555</td>
</tr>
<tr>
<td>The war against al-Qaeda is over - Kenneth Roth</td>
<td>625</td>
</tr>
<tr>
<td>Postwar - Robert M. Chesney</td>
<td>629</td>
</tr>
<tr>
<td>Law at the End of War - Deborah Pearlstein</td>
<td>653</td>
</tr>
</tbody>
</table>

## Keynote

**Cybersecurity: Countdown to Action**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Falling Prey to Cybercrime: Implications for Business and the Economy - Melissa E. Hathaway</td>
<td>725</td>
</tr>
</tbody>
</table>
Panel I:

Executive Updates on Developments in National Security Law

Moderator: Harvey Rishikof
I wish that I was here in happier times for the Intelligence Community. The last several weeks have seen a series of reckless disclosures of classified information about intelligence activities. These disclosures threaten to cause long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our Nation. And because the disclosures were made by people who did not fully understand what they were talking about, they were sensationalized and led to mistaken and misleading impressions. I hope to be able to correct some of these misimpressions today.

My speech today is prompted by disclosures about two programs that collect valuable foreign intelligence that has protected our Nation and its allies: the bulk collection of telephony metadata, and the so-called “PRISM” program. Some people claim that these disclosures were a form of “whistleblowing.” But let’s be clear. These programs are not illegal. They are authorized by Congress and are carefully overseen by the Congressional intelligence and judiciary committees. They are conducted with the approval of the Foreign Intelligence Surveillance Court and under its supervision. And they are subject to extensive, court-ordered oversight by the Executive Branch. In short, all three branches of Government knew about these programs, approved them, and helped to ensure that they complied with the law. Only time will tell the full extent of the damage caused by the unlawful disclosures of these lawful programs.

Nevertheless, I fully appreciate that it’s not enough for us simply to assert that our activities are consistent with the letter of the law. Our Government’s activities must always reflect and reinforce our core democratic values. Those of us who work in the intelligence profession share these values, including the importance of privacy. But security and privacy are not zero-sum. We have an obligation to give full meaning to both: to protect security while at the same time
Protecting privacy and other constitutional rights. But although our values are enduring, the manner in which our activities reflect those values must necessarily adapt to changing societal expectations and norms. Thus, the Intelligence Community continually evaluates and improves the safeguards we have in place to protect privacy, while at the same time ensuring that we can carry out our mission of protecting national security.

So I'd like to do three things today. First, I'd like to discuss very briefly the laws that govern intelligence collection activities. Second, I want to talk about the effect of changing technology, and the corresponding need to adapt how we protect privacy, on those collection activities. And third, I want to bring these two strands together, to talk about how some of these laws play out in practice—how we structure the Intelligence Community's collection activities under FISA to respond to these changes in a way that remains faithful to our democratic values.

II. Legal Framework

Let me begin by discussing in general terms the legal framework that governs intelligence collection activities. And it is a bedrock concept that those activities are bound by the rule of law. This is a topic that has been well addressed by others, including the general counsels of the CIA and NSA, so I will make this brief. We begin, of course, with the Constitution. Article II makes the President the Commander in Chief and gives him extensive responsibility for the conduct of foreign affairs. The ability to collect foreign intelligence derives from that constitutional source. The First Amendment protects freedom of speech. And the Fourth Amendment prohibits unreasonable searches and seizures.

I want to make a few points about the Fourth Amendment. First, under established Supreme Court rulings a person has no legally recognized expectation of privacy in information that he or she gives to a third party. So obtaining those records from the third party is not a search as to that person. I'll return to this point in a moment. Second, the Fourth Amendment doesn't apply to foreigners outside of the United States. Third, the Supreme Court has said that the "reasonableness" of a warrantless search depends on balancing the "intrusion on the individual's Fourth Amendment interests against" the search's "promotion of legitimate Governmental interests." (1)

In addition to the Constitution, a variety of statutes govern our collection activities. First, the National Security Act and a number of laws relating to specific agencies, such as the CIA Act and the NSA Act, limit what agencies can do, so that, for example, the CIA cannot engage in domestic law enforcement. We are also governed by laws such as the Electronic Communications Privacy Act, the Privacy Act and, in particular, the Foreign Intelligence Surveillance Act, or FISA. FISA was passed by Congress in 1978 and significantly amended in
PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: An Overview of Intelligence Collection by Robert S. Litt, ODNI General Counsel

2001 and 2008. It regulates electronic surveillance and certain other activities carried out for foreign intelligence purposes. I'll have much more to say about FISA later.

A final important source of legal restrictions is Executive Order 12333. This order provides additional limits on what intelligence agencies can do, defining each agency's authorities and responsibilities. In particular, Section 2.3 of EO 12333 provides that elements of the Intelligence Community "are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures . . . approved by the Attorney General . . . after consultation with" the Director of National Intelligence. These procedures must be consistent with the agencies' authorities. They must also establish strict limits on collecting, retaining or disseminating information about U.S. persons, unless that information is actually of foreign intelligence value, or in certain other limited circumstances spelled out in the order, such as to protect against a threat to life. These so-called "U.S. person rules" are basic to the operation of the Intelligence Community. They are among the first things that our employees are trained in, and they are at the core of our institutional culture.

It's not surprising that our legal regime provides special rules for activities directed at U.S. persons. So far as I know, every nation recognizes legal distinctions between citizens and non-citizens. But as I hope to make clear, our intelligence collection procedures also provide protection for the privacy rights of non-citizens.

III. Impact of Changing Societal Norms

Let me turn now to the impact of changing technology on privacy. Prior to the end of the nineteenth century there was little discussion about a "right to privacy." In the absence of mass media, photography and other technologies of the industrial age, the most serious invasions of privacy were the result of gossip or Peeping Toms. Indeed, in the 1890 article that first articulated the idea of a legal right to privacy, Louis Brandeis and Samuel Warren explicitly grounded that idea on changing technologies:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-top." (2)

Today, as a result of the way digital technology has developed, each of us shares massive amounts of information about ourselves with third parties. Sometimes this is obvious, as when
PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: An Overview of Intelligence Collection by Robert S. Litt, ODNI General Counsel

we post pictures on social media or transmit our credit card numbers to buy products online. Other times it is less obvious, as when telephone companies store records listing every call we make. All in all, there’s little doubt that the amount of data that each of us provides to strangers every day would astonish Brandeis and Warren—let alone Jefferson and Madison.

And this leads me to what I consider to be the key question. Why is it that people are willing to expose large quantities of information to private parties but don’t want the Government to have the same information? Why, for example, don’t we care if the telephone company keeps records of all of our phone calls on its servers, but we feel very differently about the prospect of the same information being on NSA servers? This does not seem to me to be a difficult question: we care because of what the Government could do with the information.

Unlike a phone company, the Government has the power to audit our tax returns, to prosecute and imprison us, to grant or deny licenses to do business, and many other things. And there is an entirely understandable concern that the Government may abuse this power. I don’t mean to say that private companies don’t have a lot of power over us. Indeed, the growth of corporate privacy policies, and the strong public reaction to the inadvertent release or commercial use of personal information, reinforces my belief that our primary privacy concern today is less with who has information than with what they do with it. But there is no question that the Government, because of its powers, is properly viewed in a different light.

On the other hand, just as consumers around the world make extensive use of modern technology, so too do potentially hostile foreign governments and foreign terrorist organizations. Indeed, we know that terrorists and weapons proliferators are using global information networks to conduct research, to communicate and to plan attacks. Information that can help us identify and prevent terrorist attacks or other threats to our security is often hiding in plain sight among the vast amounts of information flowing around the globe. New technology means that the Intelligence Community must continue to find new ways to locate and analyze foreign intelligence. We need to be able to do more than connect the dots when we happen to find them; we need to be able to find the right dots in the first place.

One approach to protecting privacy would be to limit the Intelligence Community to a targeted, focused query looking for specific information about an identified individual based on probable cause. But from the national security perspective, that would not be sufficient. The business of foreign intelligence has always been fundamentally different from the business of criminal investigation. Rather than attempting to solve crimes that have happened already, we are trying to find out what is going to happen before it happens. We may have only fragmentary information about someone who is plotting a terrorist attack, and need to find him and stop him.
We may get information that is useless to us without a store of data to match it against, such as when we get the telephone number of a terrorist and want to find out who he has been in touch with. Or we may learn about a plot that we were previously unaware of, causing us to revisit old information and find connections that we didn’t notice before—and that we would never know about if we hadn’t collected the information and kept it for some period of time. We worry all the time about what we are missing in our daily effort to protect the Nation and our allies.

So on the one hand there are vast amounts of data that contains intelligence needed to protect us not only from terrorism, but from cyber attacks, weapons of mass destruction, and good old-fashioned espionage. And on the other hand, giving the Intelligence Community access to this data has obvious privacy implications. We achieve both security and privacy protection in this context in large part by a framework that establishes appropriate controls on what the Government can do with the information it lawfully collects, and appropriate oversight to ensure that it respects those controls. The protections depend on such factors as the type of information we collect, where we collect it, the scope of the collection, and the use the Government intends to make of the information. In this way we can allow the Intelligence Community to acquire necessary foreign intelligence, while providing privacy protections that take account of modern technology.

IV. FISA Collection

In showing that this approach is in fact the way our system deals with intelligence collection, I’ll use FISA as an example for a couple of reasons. First, because FISA is an important mechanism through which Congress has legislated in the area of foreign intelligence collection. Second, because it covers a wide range of activities, and involves all three sources of law I mentioned earlier: constitutional, statutory and executive. And third, because several previously classified examples of what we do under FISA have recently been declassified, and I know people want to hear more about them.

I don’t mean to suggest that FISA is the only way we collect foreign intelligence. But it’s important to know that, by virtue of Executive Order 12333, all of the collection activities of our intelligence agencies have to be directed at the acquisition of foreign intelligence or counterintelligence. Our intelligence priorities are set annually through an interagency process. The leaders of our Nation tell the Intelligence Community what information they need in the service of the Nation, its citizens and its interests, and we collect information in support of those priorities.

I want to emphasize that the United States, as a democratic nation, takes seriously this requirement that collection activities have a valid foreign intelligence purpose. We do not use
PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: An Overview of Intelligence Collection by Robert S. Litt, ODNI General Counsel

our foreign intelligence collection capabilities to steal the trade secrets of foreign companies in order to give American companies a competitive advantage. We do not indiscriminately sweep up and store the contents of the communications of Americans, or of the citizenry of any country.

We do not use our intelligence collection for the purpose of repressing the citizens of any country because of their political, religious or other beliefs. We collect metadata—information about communications—more broadly than we collect the actual content of communications, because it is less intrusive than collecting content and in fact can provide us information that helps us more narrowly focus our collection of content on appropriate targets. But it simply is not true that the United States Government is listening to everything said by every citizen of any country.

Let me turn now to FISA. I'm going to talk about three provisions of that law: traditional FISA orders, the FISA business records provision, and Section 702. These provisions impose limits on what kind of information can be collected and how it can be collected, require procedures restricting what we can do with the information we collect and how long we can keep it, and impose oversight to ensure that the rules are followed. This sets up a coherent regime in which protections are afforded at the front end, when information is collected; in the middle, when information is reviewed and used; and at the back end, through oversight, all working together to protect both national security and privacy. The rules vary depending on factors such as the type of information being collected (and in particular whether or not we are collecting the content of communications), the nature of the person or persons being targeted, and how narrowly or broadly focused the collection is. They aren't identical in every respect to the rule that apply to criminal investigations, but I hope to persuade you that they are reasonable and appropriate in the very different context of foreign intelligence.

So let's begin by talking about traditional FISA collection. Prior to the passage of FISA in 1978, the collection of foreign intelligence was essentially unregulated by statutory law. It was viewed as a core function of the Executive Branch. In fact, when the criminal wiretap provisions were originally enacted, Congress expressly provided that they did not "limit the constitutional power of the President . . . to obtain foreign intelligence information . . . deemed essential to the national security of the United States." (3) However, ten years later, as a result of abuses revealed by the Church and Pike Committees, Congress imposed a judicial check on some aspects of electronic surveillance for foreign intelligence purposes. This is what is now codified in Title I of FISA, sometimes referred to as "traditional FISA."

FISA established a special court, the Foreign Intelligence Surveillance Court, to hear
PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: An Overview of Intelligence Collection by Robert S. Litt, ODNI General Counsel

applications by the Government to conduct electronic surveillance for foreign intelligence purposes. Because traditional FISA surveillance involves acquiring the content of communications, it is intrusive, implicating recognized privacy interests; and because it can be directed at individuals inside the United States, including American citizens, it implicates the Fourth Amendment. In FISA, Congress required that to get a “traditional” FISA electronic surveillance order, the Government must establish probable cause to believe that the target of surveillance is a foreign power or an agent of a foreign power, a probable cause standard derived from the standard used for wiretaps in criminal cases. And if the target is a U.S. person, he or she cannot be deemed an agent of a foreign power based solely on activity protected by the First Amendment—you cannot be the subject of surveillance merely because of what you believe or think.

Moreover, by law the use of information collected under traditional FISA must be subject to minimization procedures, a concept that is key throughout FISA. Minimization procedures are procedures, approved by the FISA Court, that must be “reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” (4) For example, they generally prohibit disseminating the identity of a U.S. person unless the identity itself is necessary to understand the foreign intelligence or is evidence of a crime. The reference to the purpose and technique of the particular surveillance is important. Minimization procedures can and do differ depending on the purpose of the surveillance and the technique used to implement it. These tailored minimization procedures are an important way in which we provide appropriate protections for privacy.

So let me explain in general terms how traditional FISA surveillance works in practice. Let’s say that the FBI suspects someone inside the United States of being a spy, or a terrorist, and they want to conduct electronic surveillance. While there are some exceptions spelled out in the law, such as in the case of an emergency, as a general rule they have to present an application to the FISA Court establishing probable cause to believe that the person is an agent of a foreign power, according to the statutory definition. That application, by the way, is reviewed at several levels within both the FBI and Department of Justice before it is submitted to the Court. Now, the target may have a conversation with a U.S. person that has nothing to do with the foreign intelligence purpose of the surveillance, such as talking to a neighbor about a dinner party.
PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: An Overview of Intelligence Collection by Robert S. Litt, ODNI General Counsel

Under the minimization procedures, an analyst who listens to a conversation involving a U.S. person that has no foreign intelligence value cannot generally share it or disseminate it unless it is evidence of a crime. Even if a conversation has foreign intelligence value—let’s say a terrorist is talking to a confederate—that information may only be disseminated to someone with an appropriate need to know the information pursuant to his or her mission.

In other words, electronic surveillance under FISA’s Title I implicates the well-recognized privacy interest in the contents of communications, and is subject to corresponding protections for that privacy interest—in terms of the requirements that it be narrowly targeted and that it have a substantial factual basis approved by the Court, and in terms of the limitations imposed on use of the information.

Now let me turn to the second activity, the collection of business records. After FISA was passed, it became apparent that it left some significant gaps in our intelligence collection authority. In particular, while the Government had the power in a criminal investigation to compel the production of records with a grand jury subpoena, it lacked similar authority in a foreign intelligence investigation. So a provision was added in 1998 to provide such authority, and was amended by Section 215 of the USA-PATRIOT Act passed shortly after 9/11. This provision, which is generally referred to as “Section 215,” allows us to apply to the FISA Court for an order requiring production of documents or other tangible things when they are relevant to an authorized national security investigation. Records can be produced only if they are the type of records that could be obtained pursuant to a grand jury subpoena or other court process—in other words, where there is no statutory or other protection that would prevent use of a grand jury subpoena. In some respects this process is more restrictive than a grand jury subpoena. A grand jury subpoena is issued by a prosecutor without any prior judicial review, whereas under the FISA business records provision we have to get court approval. Moreover, as with traditional FISA, records obtained pursuant to the FISA business records provision are subject to court-approved minimization procedures that limit the retention and dissemination of information about U.S. persons—another requirement that does not apply to grand jury subpoenas.

Now, of course, the FISA business records provision has been in the news because of one particular use of that provision. The FISA Court has repeatedly approved orders directing several telecommunications companies to produce certain categories of telephone metadata, such as the number calling, the number being called, and the date, time and duration of the call. It’s important to emphasize that under this program we do not get the content of any conversation; we do not get the identity of any party to the conversation; and we do not get any cell site or GPS locational information.
PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: An Overview of Intelligence Collection by Robert S. Litt, ODNI General Counsel

The limited scope of what we collect has important legal consequences. As I mentioned earlier, the Supreme Court has held that if you have voluntarily provided this kind of information to third parties, you have no reasonable expectation of privacy in that information. All of the metadata we get under this program is information that the telecommunications companies obtain and keep for their own business purposes. As a result, the Government can get this information without a warrant, consistent with the Fourth Amendment.

Nonetheless, I recognize that there is a difference between getting metadata about one telephone number and getting it in bulk. From a legal point of view, Section 215 only allows us to get records if they are "relevant" to a national security investigation, and from a privacy perspective people worry that, for example, the government could apply data mining techniques to a bulk data set and learn new personal facts about them—even though the underlying set of records is not subject to a reasonable expectation of privacy for Fourth Amendment purposes.

On the other hand, this information is clearly useful from an intelligence perspective: It can help identify links between terrorists overseas and their potential confederates in the United States. It’s important to understand the problem this program was intended to solve. Many will recall that one of the criticisms made by the 9/11 Commission was that we were unable to find the connection between a hijacker who was in California and an al-Qaida safe house in Yemen. Although NSA had collected the conversations from the Yemen safe house, they had no way to determine that the person at the other end of the conversation was in the United States, and hence to identify the homeland connection. This collection program is designed to help us find those connections.

In order to do so, however, we need to be able to access the records of telephone calls, possibly going back many years. However, telephone companies have no legal obligation to keep this kind of information, and they generally destroy it after a period of time determined solely by their own business purposes. And the different telephone companies have separate datasets in different formats, which makes analysis of possible terrorist calls involving several providers considerably slower and more cumbersome. That could be a significant problem in a fast-moving investigation where speed and agility are critical, such as the plot to bomb the New York City subways in 2009.

The way we fill this intelligence gap while protecting privacy illustrates the analytical approach I outlined earlier. From a subscriber’s point of view, as I said before, the difference between a telephone company keeping records of his phone calls and the Intelligence Community keeping the same information is what the Government could do with the records. That’s an entirely legitimate concern. We deal with it by limiting what the Intelligence Community is allowed do with the information we get under this program—limitations that are approved by the FISA Court:
First, we put this information in secure databases.

Second, the only intelligence purpose for which this information can be used is counterterrorism.

Third, we allow only a limited number of specially trained analysts to search these databases.

Fourth, even those trained analysts are allowed to search the database only when they have a reasonable and articulable suspicion that a particular telephone number is associated with particular foreign terrorist organizations that have been identified to the Court. The basis for that suspicion has to be documented in writing and approved by a supervisor.

Fifth, they're allowed to use this information only in a limited way, to map a network of telephone numbers calling other telephone numbers.

Sixth, because the database contains only metadata, even if the analyst finds a previously unknown telephone number that warrants further investigation, all she can do is disseminate the telephone number. She doesn't even know whose number it is. Any further investigation of that number has to be done pursuant to other lawful means, and in particular, any collection of the contents of communications would have to be done using another valid legal authority, such as a traditional FISA.

Finally, the information is destroyed after five years.

The net result is that although we collect large volumes of metadata under this program, we only look at a tiny fraction of it, and only for a carefully circumscribed purpose—to help us find links between foreign terrorists and people in the United States. The collection has to be broad to be operationally effective, but it is limited to non-content data that has a low privacy value and is not protected by the Fourth Amendment. It doesn't even identify any individual. Only the narrowest, most important use of this data is permitted; other uses are prohibited. In this way, we protect both privacy and national security.

Some have questioned how collection of a large volume of telephone metadata could comply with the statutory requirement that business records obtained pursuant to Section 215 be "relevant to an authorized investigation." While the Government is working to determine what additional information about the program can be declassified and disclosed, including the actual court papers, I can give a broad summary of the legal basis. First, remember that the "authorized investigation" is an intelligence investigation, not a criminal one. The statute requires that an authorized investigation be conducted in accordance with guidelines approved by the Attorney General, and those guidelines allow the FBI to conduct an investigation into a
foreign terrorist entity if there is an “articulable factual basis . . . that reasonably indicates that the [entity] may have engaged in . . . international terrorism or other threat to the national security,” or may be planning or supporting such conduct. (5) In other words, we can investigate an organization, not merely an individual or a particular act, if there is a factual basis to believe the organization is involved in terrorism. And in this case, the Government’s applications to collect the telephony metadata have identified the particular terrorist entities that are the subject of the investigations.

Second, the standard of “relevance” required by this statute is not the standard that we think of in a civil or criminal trial under the rules of evidence. The courts have recognized in other contexts that “relevance” can be an extremely broad standard. For example, in the grand jury context, the Supreme Court has held that a grand jury subpoena is proper unless “there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.” (6) And in civil discovery, relevance is “construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case.” (7)

In each of these contexts, the meaning of “relevance” is sufficiently broad to allow for subpoenas or requests that encompass large volumes of records in order to locate within them a smaller subset of material that will be directly pertinent to or actually be used in furtherance of the investigation or proceedings. In other words, the requester is not limited to obtaining only those records that actually are potentially incriminating or pertinent to establishing liability, because to identify such records, it is often necessary to collect a much broader set of the records that might potentially bear fruit by leading to specific material that could bear on the issue.

When it passed the business records provision, Congress made clear that it had in mind such broad concepts of relevance. The telephony metadata collection program meets this relevance standard because, as I explained earlier, the effectiveness of the queries allowed under the strict limitations imposed by the court—the queries based on “reasonable and articulable suspicion”—depends on collecting and maintaining the data from which the narrowly focused queries can be made. As in the grand jury and civil discovery contexts, the concept of “relevance” is broad enough to allow for the collection of information beyond that which ultimately turns out to be important to a terrorist-related investigation. While the scope of the collection at issue here is broader than typically might be acquired through a grand jury subpoena or civil discovery request, the basic principle is similar: the information is relevant because you need to have the broader set of records in order to identify within them the information that is actually important to a terrorism investigation. And the reasonableness of this
method of collection is reinforced by the all of the stringent limitations imposed by the Court to ensure that the data is used only for the approved purpose.

I want to repeat that the conclusion that the bulk metadata collection is authorized under Section 215 is not that of the Intelligence Community alone. Applications to obtain this data have been repeatedly approved by numerous judges of the FISA Court, each of whom has determined that the application complies with all legal requirements. And Congress reauthorized Section 215 in 2011, after the Intelligence and Judiciary Committees of both Houses had been briefed on the program, and after information describing the program had been made available to all Members. In short, all three branches of Government have determined that this collection is lawful and reasonable—in large part because of the substantial protections we provide for the privacy of every person whose telephone number is collected.

The third program I want to talk about is Section 702, part of the FISA Amendments Act of 2008. Again, a little history is in order. Generally speaking, as I said before, Title I of FISA, or traditional FISA, governs electronic surveillance conducted within the United States for foreign intelligence purposes. When FISA was first passed in 1978, Congress did not intend it to regulate the targeting of foreigners outside of the United States for foreign intelligence purposes.

This kind of surveillance was generally carved out of coverage under FISA by the way Congress defined "electronic surveillance." Most international communications in 1978 took place via satellite, so Congress excluded international radio communications from the definition of electronic surveillance covered by FISA, even when the radio waves were intercepted in the United States, unless the target of the collection was a U.S. person in the United States.

Over time, that technology-based differentiation fell apart. By the early twenty-first century, most international communications travelled over fiber optic cables and thus were no longer "radio communications" outside of FISA's reach. At the same time there was a dramatic increase in the use of the Internet for communications purposes, including by terrorists. As a result, Congress's original intention was frustrated; we were increasingly forced to go to the FISA Court to get individual warrants to conduct electronic surveillance of foreigners overseas for foreign intelligence purposes.

After 9/11, this burden began to degrade our ability to collect the communications of foreign terrorists. Section 702 created a new, more streamlined procedure to accomplish this surveillance. So Section 702 was not, as some have called it, a "defanging" of the FISA Court's traditional authority. Rather, it extended the FISA Court's oversight to a kind of surveillance that Congress had originally placed outside of that oversight: the surveillance, for
foreign intelligence purposes, of foreigners overseas. This American regime imposing judicial supervision of a kind of foreign intelligence collection directed at citizens of other countries is a unique limitation that, so far as I am aware, goes beyond what other countries require of their intelligence services when they collect against persons who are not their own citizens.

The privacy and constitutional interests implicated by this program fall between traditional FISA and metadata collection. On the one hand we are collecting the full content of communications; on the other hand we are not collecting information in bulk and we are only targeting non-U.S. persons for valid foreign intelligence purposes. And the information involved is unquestionably of great importance for national security: collection under Section 702 is one of the most valuable sources of foreign intelligence we have. Again, the statutory scheme, and the means by which we implement it, are designed to allow us to collect this intelligence, while providing appropriate protections for privacy. Collection under Section 702 does not require individual judicial orders authorizing collection against each target. Instead, the FISA Court approves annual certifications submitted by the Attorney General and the Director of National Intelligence that identify categories of foreign intelligence that may be collected, subject to Court-approved “targeting” procedures and “minimization” procedures.

The targeting procedures are designed to ensure that we target someone only if we have a valid foreign intelligence purpose; that we target only non-U.S. persons reasonably believed to be outside of the United States; that we do not intercept wholly domestic communications; and that we do not target any person outside the United States as a “back door” means of targeting someone inside the United States. The procedures must be reviewed by the Court to ensure that they are consistent with the statute and the Fourth Amendment. In other words, the targeting procedures are a way of minimizing the privacy impact of this collection both as to Americans and as to non-Americans by limiting the collection to its intended purpose.

The concept of minimization procedures should be familiar to you by now: they are the procedures that limit the retention and dissemination of information about U.S. persons. We may incidentally acquire the communications of Americans even though we are not targeting them, for example if they talk to non-U.S. persons outside of the United States who are properly targeted for foreign intelligence collection. Some of these communications may be pertinent; some may not be. But the incidental acquisition of non-pertinent information is not unique to Section 702. It is common whenever you lawfully collect information, whether it's by a criminal wiretap (where the target's conversations with his friends or family may be intercepted) or when we seize a terrorist's computer or address book, either of which is likely to contain non-pertinent information. In passing Section 702, Congress recognized this reality and required us to establish procedures to minimize the impact of this incidental collection on privacy.
PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: An Overview of Intelligence Collection by Robert S. Litt, ODNI General Counsel

How does Section 702 work in practice? As of today, there are certifications for several different categories of foreign intelligence information. Let’s say that the Intelligence Community gets information that a terrorist is using a particular email address. NSA analysts look at available data to assess whether that email address would be a valid target under the statute—whether the email address belongs to someone who is not a U.S. person, whether the person with the email address is outside the United States, and whether targeting that email address is likely to lead to the collection of foreign intelligence relevant to one of the certifications. Only if all three requirements of the statute are met, and validated by supervisors, will the email address be approved for targeting. We don’t randomly target email addresses or collect all foreign individuals’ emails under Section 702; we target specific accounts because we are looking for foreign intelligence information. And even after a target is approved, the court approved procedures require NSA to continue to verify that its targeting decision is valid based on any new information.

Any communications that we collect under Section 702 are placed in secure databases, again with limited access. Trained analysts are allowed to use this data for legitimate foreign intelligence purposes, but the minimization procedures require that if they review a communication that they determine involves a U.S. person or information about a U.S. person, and they further determine that it has no intelligence value and is not evidence of a crime, it must be destroyed. In any case, conversations that are not relevant are destroyed after a maximum of five years. So under Section 702, we have a regime that involves judicial approval of procedures that are designed to narrow the focus of the surveillance and limit its impact on privacy. I’ve outlined three different collection programs, under different provisions of FISA, which all reflect the framework I described. In each case, we protect privacy by a multi-layered system of controls on what we collect and how we use what we collect, controls that are based on the nature and intrusiveness of the collection, but that take into account the ways in which that collection can be useful to protect national security. But we don’t simply set out a bunch of rules and trust people to follow them. There are substantial safeguards in place that help ensure that the rules are followed.

These safeguards operate at several levels. The first is technological. The same technological revolution that has enabled this kind of intelligence collection and made it so valuable also allows us to place relatively stringent controls on it. For one thing, intelligence agencies can work with providers so that they provide the information we are allowed to acquire under the relevant order, and not additional information. Second, we have secure databases to hold this data, to which only trained personnel have access. Finally, modern information security techniques allow us to create an audit trail tracking who uses these databases and how, so that we have a record that can enable us to identify any possible misuse. And I want to emphasize that there’s no indication so far that anyone has defeated those technological controls and
improperly gained access to the databases containing people's communications. Documents such as the leaked secondary order are kept on other NSA databases that do not contain this kind of information, to which many more NSA personnel have access.

We don't rely solely on technology. NSA has an internal compliance officer, whose job includes developing processes that all NSA personnel must follow to ensure that NSA is complying with the law. In addition, decisions about what telephone numbers we use as a basis for searching the telephone metadata are reviewed first within NSA, and then by the Department of Justice. Decisions about targeting under Section 702 are reviewed first within NSA, and then by the Department of Justice and by my agency, the Office of the Director of National Intelligence, which has a dedicated Civil Liberties Protection Officer who actively oversees these programs. For Title I collection, the Department of Justice regularly conducts reviews to ensure that information collected is used and disseminated in accordance with the court-approved minimization procedures. Finally, independent Inspectors General also review the operation of these programs. The point is not that these individuals are perfect; it's that as you have more and more people from more and more organizations overseeing the operation of the programs, it becomes less and less likely that unintentional errors will go unnoticed or that anyone will be able to misuse the information.

But wait, there's more. In addition to this oversight by the Executive Branch, there is considerable oversight by both the FISA Court and the Congress. As I've said, the FISA Court has to review and approve the procedures by which we collect intelligence under FISA, to ensure that those procedures comply with the statute and the Fourth Amendment. In addition, any compliance matter, large or small, has to be reported to the Court. Improperly collected information generally must be deleted, subject only to some exceptions set out in the Court's orders, and corrective measures are taken and reported to the Court until it is satisfied.

And I want to correct the erroneous claim that the FISA Court is a rubber stamp. Some people assume that because the FISA Court approves almost every application, it does not give these applications careful scrutiny. In fact the exact opposite is true. The judges and their professional staff review every application carefully, and often ask extensive and probing questions, seek additional information, or request changes, before the application is ultimately approved. Yes, the Court approves the great majority of applications at the end of this process, but before it does so, its questions and comments ensure that the application complies with the law.

Finally, there is the Congress. By law, we are required to keep the Intelligence and Judiciary Committees informed about these programs, including detailed reports about their operation and compliance matters. We regularly engage with them and discuss these authorities, as we did this week, to provide them information to further their oversight responsibilities. For example,
when Congress reauthorized Section 215 in 2009 and 2011 and Section 702 in 2012, information was made available to every member of Congress, by briefings and written material, describing these programs in detail.

* * *

In short, the procedures by which we implement collection under FISA are a sensible means of accounting for the changing nature of privacy in the information age. They allow the Intelligence Community to collect information that is important to protect our Nation and its allies, while protecting privacy by imposing appropriate limits on the use of that information. Much is collected, but access, analysis and dissemination are subject to stringent controls and oversight. This same approach—making the extent and nature of controls over the use of information vary depending on the nature and sensitivity of the collection—is applied throughout our intelligence collection.

And make no mistake, our intelligence collection has helped to protect our Nation from a variety of threats—and not only our Nation, but the rest of the world. We have robust intelligence relationships with many other countries. These relationships go in both directions, but it is important to understand that we cannot use foreign intelligence to get around the limitations in our laws, and we assume that our other countries similarly expect their intelligence services to operate in compliance with their own laws. By working closely with other countries, we have helped ensure our common security. For example, while many of the details remain classified, we have provided the Congress a list of 54 cases in which the bulk metadata and Section 702 authorities have given us information that helped us understand potential terrorist activity and even disrupt it, from potential bomb attacks to material support for foreign terrorist organizations. Forty-one of these cases involved threats in other countries, including 25 in Europe. We were able to alert officials in these countries to these events, and help them fulfill their mission of protecting their nations, because of these capabilities.

I believe that our approach to achieving both security and privacy is effective and appropriate. It has been reviewed and approved by all three branches of Government as consistent with the law and the Constitution. It is not the only way we could regulate intelligence collection, however. Even before the recent disclosures, the President said that we welcomed a discussion about privacy and national security, and we are working to declassify more information about our activities to inform that discussion. In addition, the Privacy and Civil Liberties Oversight Board—an independent body charged by law with overseeing our counterterrorism activities—has announced that it intends to provide the President and Congress a public report on the Section 215 and 702 programs, including the collection of bulk metadata. The Board met recently with the President, who welcomed their review and committed to providing them access to all materials they will need to fulfill their oversight and advisory functions. We look forward to
working with the Board on this important project.

This discussion can, and should, have taken place without the recent disclosures, which have brought into public view the details of sensitive operations that were previously discussed on a classified basis with the Congress and in particular with the committees that were set up precisely to oversee intelligence operations. The level of detail in the current public debate certainly reflects a departure from the historic understanding that the sensitive nature of intelligence operations demanded a more limited discussion. Whether or not the value of the exposure of these details outweighs the cost to national security is now a moot point. As the debate about our surveillance programs goes forward, I hope that my remarks today have helped provide an appreciation of the efforts that have been made—and will continue to be made—to ensure that our intelligence activities comply with our laws and reflect our values.

Thank you.


(2) Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 195 (1890)

(3) 82 Stat. 214, formerly codified at 18 U.S.C. § 2511(3)

(4) See, e.g., 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A)

(5) Attorney General's Guidelines for Domestic FBI Operations (2008), at 23


Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Grassley:

On July 29, 2013, the Foreign Intelligence Surveillance Court (FISC) corresponded with the Senate Judiciary Committee in a response to questions about the Court’s practices (copy enclosed). In our response, we explained in greater detail the process by which the Court interacts with the executive branch. Among other things, we noted:

The annual statistics provided to Congress by the Attorney General pursuant to 50 U.S.C. §§ 1807 and 1862(b) – frequently cited to in press reports as a suggestion that the Court’s approval rate of applications is over 99% – reflect only the number of final applications submitted to and acted on by the Court. These statistics do not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them.

Our letter also stated, “In a typical week, the Court seeks additional information or modifies the terms proposed by the government in a significant percentage of cases.” We further indicated that the FISC was then just beginning a practice of collecting statistics on the rate at which such modifications occur. We are now ready to provide some initial statistics in this regard.

During the three month period from July 1, 2013 through September 30, 2013, we have observed that 24.4% of matters submitted ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action. This does not include, for example, mere typographical corrections. Although we have every reason to believe that this three month period is typical in terms of the historic rate of modifications, we will continue to collect these statistics for an additional period of time and we will inform you if those data suggest that the recent three months were anomalous. It should be noted, however, that these statistics are an attempt to measure the results of what are, typically, informal communications between the branches. Therefore, the determination of exactly when a
modification is "substantial," and whether it was caused solely by the FISC's intervention, can be a judgment call.

We hope this information is helpful to Congress and the public in better understanding the role and operations of the FISC.

Sincerely,

Reggie B. Walton
Presiding Judge

Enclosure

Identical letters sent to:

Honorable Patrick J. Leahy
Honorable Bob Goodlatte
Honorable John Conyers, Jr.
Honorable Dianne Feinstein
Honorable Saxby Chambliss
Honorable Mike Rogers
Honorable C. A. Dutch Ruppersberger
July 29, 2013

Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Grassley:

I am writing in response to your letter of July 18, 2013, in which you posed several questions about the operations of the Foreign Intelligence Surveillance Court (the Court). As you requested, we are providing unclassified responses. We would note that, as a general matter, the Court’s practices have evolved over time. Various developments in the last several years—including statutory changes, changes in the size of the Court and its staff, the adoption of new Rules of Procedure in 2010, and the relocation of the Court’s facilities from the Department of Justice headquarters to a secure space in the federal courthouse in 2009—have affected some of these practices. The responses below reflect the current practices of the Court.

1. Describe the typical process that the Court follows when it considers the following: (1) an application for an order for electronic surveillance under Title I of FISA; (2) an application for an order for access to business records under Title V of FISA; and (3) submissions from the government under Section 702 of FISA. As to applications for orders for access to business records under Title V of FISA, please describe whether the process for the Court’s consideration of such applications is different when considering requests for bulk collection of phone call metadata records, as recently declassified by the Director of National Intelligence.

Each week, one of the eleven district court judges who comprise the Court is on duty in Washington. As discussed below, most of the Court’s work is handled by the duty judge with the assistance of attorneys and clerk’s office personnel who staff the Court. Some of the Court’s more complex or time-consuming matters are handled by judges outside of the duty-week system, at the discretion of the Presiding Judge. In either case, matters before the Court are thoroughly reviewed and analyzed by the Court.

Rule 9(a) of the United States Foreign Intelligence Surveillance Court Rules of Procedure
Honorable Charles E. Grassley  
July 29, 2013  
Page 2

(FISC Rules of Procedure) \(^1\) requires that except in certain circumstances (i.e., a submission pursuant to an emergency authorization under the statute or as otherwise permitted by the Court), a proposed application must be submitted by the government no later than seven days before the government seeks to have the matter entertained. \(^2\) Upon the Court’s receipt of a proposed application for an order under FISA, a member of the Court’s legal staff reviews the application and evaluates whether it meets the legal requirements under the statute. As part of this evaluation, a Court attorney will often have one or more telephone conversations with the government\(^3\) to seek additional information and/or raise concerns about the application. A Court attorney then prepares a written analysis of the application for the duty judge, which includes an identification of any weaknesses, flaws, or other concerns. For example, the attorney may recommend that the judge consider requiring the addition of information to the application; imposing special reporting requirements; \(^4\) or shortening the requested duration of an authorization.

The judge then reviews the proposed application, as well as the attorney’s written analysis. \(^3\) The judge typically makes a preliminary determination at that time about what course

---

\(^1\) A copy of the FISC Rules of Procedure is appended hereto as Attachment A. The rules are also available at http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

\(^2\) A proposed application is also sometimes referred to as a “read copy” and has been referred to in this manner in at least one recent congressional hearing. A proposed application or “read copy” is a near-final version of the government’s application, which does not include the signatures of executive branch officials required by statutory provisions such as 50 U.S.C. §§ 1804(a)(6) and 1823(a)(6). As described below, in most circumstances, the government will subsequently file a final copy of an application pursuant to Rule 9(b) of the FISC Rules of Procedure. Both the proposed and final applications include proposed orders.

The process of using proposed applications and final applications is altogether similar to the process employed by other federal courts in considering applications for wiretap orders under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (“Title III”), which is codified at 18 U.S.C. §§ 2510-2522.

\(^3\) In discussing Court interactions with “the government” throughout this document, I am referring to interactions with attorneys in the Office of Intelligence of the National Security Division of the United States Department of Justice.

\(^4\) Pursuant to 50 U.S.C. §§ 1805(d)(3) and 1824(d)(3), the Court is authorized to assess compliance with the statutorily-required minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

\(^5\) For each application, the Court retains the attorney’s written analysis and the notes made by the judge, so that if the government later seeks to renew the authorization, the judge who considers the next
of action to take. These courses of action might include indicating to Court staff that he or she is prepared to approve the application without a hearing; indicating an inclination to impose conditions on the approval of the application; determining that additional information is needed about the application; or determining that a hearing would be appropriate before deciding whether to grant the application. A staff attorney will then relay the judge’s inclination to the government, and the government will typically proceed by providing additional information, or by submitting a final application (sometimes with amendments, at the government’s election) for the Court’s ruling pursuant to Rule 9(b) of the FISC Rules of Procedure. In conjunction with its submission of a final application, the government has an opportunity to request a hearing, even if the judge did not otherwise intend to require one. The government might request a hearing, for example, to challenge conditions that the judge has indicated he or she would impose on the approval of an application. If the judge schedules a hearing, the judge decides whether to approve the application thereafter. Otherwise, the judge makes a determination based on the final written application submitted by the government. In approving an application, a judge will sometimes issue a Supplemental Order in addition to signing the government’s proposed orders. Often, a Supplemental Order imposes some form of reporting requirement on the government.

If after receiving a final application, the judge is inclined to deny it, the Court will prepare a statement of reason(s) pursuant to 50 U.S.C. § 1803(a)(1). In some cases, the government may decide not to submit a final application, or to withdraw one that has been submitted, after learning that the judge does not intend to approve it. The annual statistics provided to Congress by the Attorney General pursuant to 50 U.S.C. §§ 1807 and 1862(b) – frequently cited to in press reports as a suggestion that the Court’s approval rate of applications is over 99% – reflect only the number of final applications submitted to and acted on by the Court. These statistics do not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them.6

Most applications under Title V of FISA are handled pursuant to the process described above. However, applications under Title V of FISA for bulk collection of phone call metadata records are normally handled by the weekly duty judge using a process that is similar to the one described above, albeit more exacting. The government typically submits a proposed application of this type more than one week in advance. The attorney who reviews the application spends a

application has the benefit of the prior thoughts of the judge(s) and staff, and a written record of any problems with the case.

6 Notably, the approval rate for Title III wiretap applications (see note 2 above) is higher than the approval rate for FISA applications, even using the Attorney General’s FISA statistics as the baseline for comparison, as recent statistics show that from 2008 through 2012, only five of 13,593 Title III wiretap applications were requested but not authorized. See Administrative Office of the United States Courts, Wiretap Report 2012, Table 7 (available at http://www.uscourts.gov/uscourts/statistics/wiretapreports/2012/Table7.pdf).
greater amount of time reviewing and preparing a written analysis of such an application, in part because the Court has always required detailed information about the government’s implementation of this authority. The judge likewise typically spends a greater amount of time than he or she normally spends on an individual application, carefully considering the extensive information provided by the government and determining whether to seek more information or hold a hearing before ruling on the application.

As described above, the majority of applications submitted to the Court are handled on a seven-day cycle, by a judge sitting on a weekly duty schedule. Applications that are novel or more complex are sometimes handled on a longer time-line, usually require additional briefing, and are assigned by the Presiding Judge based on judges’ availability. Section 702 (i.e., 50 U.S.C. § 1881a) applications would typically fall into this category.

Where the Court’s process for handling Section 702 applications differs from the process described above, it is largely based on the statutory requirements of that section, which was enacted as part of the FISA Amendments Act of 2008 (FAA). Pursuant to 50 U.S.C. §§ 1881a(g)(1)(A) & (g)(2)(D)(i), prior to the implementation of an authorization under Section 702, the Attorney General and the Director of National Intelligence must provide the Court with a written certification containing certain statutorily required elements, and that certification must include an effective date for the authorization that is at least 30 days after the submission of the written certification to the Court. Under 50 U.S.C. § 1881a(i)(B), the Court must review the certification, as well as the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e), not later than 30 days after the date on which the certification and procedures are submitted. The statutorily-imposed deadline for the Court’s review typically coincides with the effective date identified in the final certification filed with the Court.

The government’s submission of a Section 702 application typically includes a cover filing that highlights any special issues and identifies any changes that have been made relative to the prior application. The government has typically filed proposed (read copy) Section 702 applications approximately one month before filing a final application. Proposed Section 702 applications are reviewed by multiple members of the Court’s legal staff. At the direction of the Presiding Judge or a judge who has been assigned to handle the Section 702 application, the

---

7 "Section 702 application" is used here to refer collectively to a Section 702 certification and supporting affidavit, as well as to the statutorily-required targeting and minimization procedures.

8 If the acquisition has already begun (e.g., pursuant to a determination of exigent circumstances under 50 U.S.C. § 1881a(c)(2)) or the effective date is less than 30 days after the submission of the written certification to the Court (e.g., because of an amendment to a certification while judicial review is pending, pursuant to 50 U.S.C. § 1881a(i)(1)(C)), 50 U.S.C. § 1881a(g)(2)(D)(ii) requires the certification to include the date the acquisition began or the effective date of the authorization.
Honorable Charles E. Grassley  
July 29, 2013  
Page 5

Court’s legal staff may request a meeting with the government to discuss a proposed application. Also at the direction of the Presiding Judge or a judge who has been assigned to handle the Section 702 application, the Court legal staff may request additional information from the government or convey a judge’s concerns about the legal sufficiency of a proposed Section 702 application. Following these interactions, the government files a final Section 702 application, which the government may have elected to amend based on any concerns raised by the judge.

The judge reviews the final Section 702 application and may set a hearing if he or she has additional questions about it. If the judge finds (based on the written submission alone or the written submission in combination with a hearing) that the certification contains all of the required elements, and that the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States, the judge enters an order approving the certification in accordance with 50 U.S.C. § 1881a(i)(3)(A). As required by 50 U.S.C. § 1881a(i)(3)(C), the judge also issues an opinion in support of the order. If the judge finds that the certification does not contain the required elements or the targeting and minimization procedures are inconsistent with the requirements of 50 U.S.C. §§ 1881a(d) & (e), or the Fourth Amendment, the judge will, pursuant to 50 U.S.C. § 1881a(i)(3)(B), issue an order directing the government to, at the government’s election and to the extent required by the Court’s order, either correct any deficiency identified by the Court’s order not later than 30 days after the date on which the Court issues the order, or cease, or not begin, the implementation of the authorization for which the certification was submitted. Subsequent review of any remedial measures taken by the government may then be required and may result in another order and opinion pursuant to 50 U.S.C. § 1881a(i).

2. When considering such applications and submissions, please describe the interaction between the government and the Court (including both judges and court staff), including any hearings, meetings, or other means through which the Court has the opportunity to ask questions or seek additional information from the government. Please describe how frequently such exchanges occur, and generally what types of additional information that the Court might request of the government, if any. Please also describe how frequently the Court asks the government to make changes to its applications and submissions before ruling.

The process through which the Court interacts with the government in reviewing proposed applications, seeking additional information, conveying Court concerns, and adjudicating final applications, is very similar to the process employed by other federal courts in considering applications for wiretap orders under Title III (discussed in notes 2 and 6 above).

Under FISA practice, the first set of interactions often take place at the staff level. The Court’s legal staff frequently interacts with the government in various ways in the context of
examining the legal sufficiency of applications before they are presented in final form to a judge. Indeed, in the process of reviewing the government’s applications and submissions in order to provide advice to the judge, the legal staff interact with the government on a daily basis. These daily interactions typically consist of secure telephone conversations in which legal staff ask the government questions about the legal and factual elements of applications or submissions. These questions may originate with legal staff after an initial review of an application or submission, or they may come from a judge.

At the direction of the Presiding Judge or the judge assigned to a matter, Court legal staff sometimes meet with the government in connection with applications and submissions. The Court typically requests such meetings when a proposed application or submission presents a special legal or factual concern about which the Court would like additional information (e.g., a novel use of technology or a request to use a new surveillance or search technique). The frequency of such meetings varies depending on the Court’s assessment of its need for additional information in matters before it and the most conducive means to obtain that information. Court legal staff may meet with the government as often as 2-3 times a week, or as few as 1-2 times a month, in connection with the various matters pending before the Court.

Pursuant to 50 U.S.C. § 1803(a)(2)(A) and Rule 17(a) of the FISC Rules of Procedure, the Court also holds hearings in cases in which a judge assesses that he or she needs additional information in order to rule on a matter. The frequency of hearings varies depending on the nature and complexity of matters pending before the Court at a given time, and also, to some extent, based on the individual preferences of different judges. Hearings are attended, at a minimum, by the Department of Justice attorney who prepared the application and a fact witness from the agency seeking the Court’s authorization.

The types of additional information sought from the government — through telephone conversations, meetings, or hearings — include, but are not limited to, the following: additional facts to justify the government’s belief that its application meets the legal requirements for the type of authority it is seeking (e.g., in the case of electronic surveillance, that might include additional information to justify the government’s belief that a target of surveillance is a foreign power or an agent of a foreign power, as required by 50 U.S.C. § 1804(a)(3)(A), or that the target is using or about to use a particular facility, as required by 50 U.S.C. § 1804(a)(3)(B)); additional facts about how the government intends to implement statutorily required minimization procedures (see, e.g., 50 U.S.C. §§ 1801(h); 1805(a)(3); 1824(a)(3); 1861(c)(1); 1881a(i)(3)(A); and 1881o(c)(1)(c)); additional information about the government’s prior implementation of a Court order, particularly if the government has previously failed to comply fully with a Court order; or additional information about novel issues of technology or law (see Rule 11 of FISC Rules of Procedure).

In a typical week, the Court seeks additional information or modifies the terms proposed
by the government in a significant percentage of cases. (The Court has recently initiated the process of tracking more precisely how frequently this occurs.) The judge may determine, for example, that he or she cannot make the necessary findings under the statute without the addition of information to the application, or that he or she can approve only some of the authorities sought through the application. The government then has the choice to alter its final application or proposed orders in response to the judge’s concerns; request a hearing to address those concerns; submit a final application without changes; or elect not to proceed at all with a final application. If the government files a final application, the Court may, on its own, make changes to the government’s proposed orders (or issue totally redrafted orders) to address the judge’s concern about a given application. The judge may choose, for example, to make an authorization of a shorter duration than what was requested by the government, or the judge may issue a Supplemental Order imposing special reporting or minimization requirements on the government’s implementation of an authorization.

3. Public FISA Court opinions and orders make clear that the Court has considered the views of non-governmental parties in certain cases, including a provider challenge to the Protect America Act of 2007. Describe instances where nongovernmental parties have appeared before the Court. Has the Court invited or heard views from a nongovernmental party regarding applications or submissions under Title I, Title V, or Title VII of FISA? If so, how did this come about, and what was the process or mechanism that the Court used to enable such views to be considered?

FISA does not provide a mechanism for the Court to invite the views of nongovernmental parties. In fact, the Court’s proceedings are ex parte as required by the statute (see, e.g., 50 U.S.C. §§ 1805(a), 1824(a), 1842(d)(1) & 1861(c)(1)), and in keeping with the procedures followed by other courts in applications for search warrants and wiretap orders. Nevertheless, the statute and the FISC Rules of Procedure provide multiple opportunities for recipients of Court orders or government directives to challenge those orders or directives, either directly or through refusal to comply with orders or directives. Additionally, as detailed below, there have been several instances – particularly in the past several months – in which nongovernmental parties have appeared before the Court outside of the context of a challenge to an individual Court order or government directive.

There has been one instance in which the Court heard arguments from a nongovernmental party that sought to substantively contest a directive from the government. Specifically, in 2007, the government issued directives to Yahoo!, Inc. (Yahoo) pursuant to Section 105B of the Protect America Act of 2007 (PAA). Yahoo refused to comply with the directives, and the government

---

9 This assessment does not include minor technical or typographical changes, which occur more frequently.
filed a motion with this Court to compel compliance. The Court ordered and received briefing from both parties, and rendered a decision in April 2008.\(^\text{10}\)

As noted above, the FISC Rules of Procedure and the FISA statute provide opportunities for the appearance of nongovernmental parties before the Court in matters pending pursuant to Titles I, V and VII of the statute. For example, Rule 19(a) of the FISC Rules of Procedure provides that if a person or entity served with a Court order fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly. Thus, a nongovernmental party served with an order may invite an opportunity to be heard by the Court through refusal to comply with an order.

With respect to applications filed under Title V of FISA, 50 U.S.C. § 1861(3)(2)(A)(i) provides that a person receiving a production order may challenge the legality of that order by filing a petition with the Court. The same section of the statute provides that the recipient of a production order may challenge the non-disclosure order imposed in connection with a production order by filing a petition to modify or set aside the nondisclosure order. Rules 33-36 of the FISC Rules of Procedure delineate the procedures and requirements for filing such petitions, including the time limits on such challenges. To date, no recipient of a production order has opted to invoke this section of the statute.

With respect to applications filed under Title VII of FISA, 50 U.S.C. § 1881a(h)(4)(A) provides that an electronic communication service provider who receives a directive pursuant to Section 702 may file a petition to modify or set aside the directive with the Court. Sections 1881a(h)(4)(A)-(G) of the statute, as well as Rule 28 of the FISC Rules of Procedure, delineate

\(^{10}\) Yahoo thereafter appealed the Court's decision to the Foreign Intelligence Surveillance Court of Review (FISCR). See In re Directives (redacted) Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008). This is not the only instance in which a nongovernmental entity has appeared before the FISCR. In 2002, the FISCR accepted briefs filed by the ACLU and the National Association of Criminal Defense Lawyers as amici curiae in In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

While Yahoo's identity as the provider that challenged these directives was previously under seal pursuant to the FISCR's decision in In re Directives, 551 F.3d 1004, 1016-18, the FISCR issued an Order on June 26, 2013, indicating that it does not object to the release of Yahoo's identity, and ordering, among other things, a new declassification review of the FISCR's opinion in In re Directives. The FISCR issued this order in response to a motion by Yahoo's counsel, and after receiving briefing by Yahoo and the government. Yahoo also recently filed a motion for publication of the Court's decision that was appealed to the FISCR, resulting in the published opinion in In re Directives. The Court granted the motion. Documents related to Yahoo's recent motion to this Court are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html under Docket No. 105B(g) 07-01.
the procedures and requirements for such challenges. Relatively, 50 U.S.C. § 1881a(h)(5)(A) provides that if an electronic communication service provider fails to comply with a directive issued under Section 702, the Attorney General may file a petition with the Court for an order to compel compliance, which would likely result in the service provider’s appearance before the Court through its legal representatives. (Section 1881a(h)(5), as well as Rule 29 of the FISC Rules of Procedure, provide further detail on the procedures and requirements for the enforcement of Section 702 directives.) Finally, 50 U.S.C. § 1881a(h)(6) and Rule 31 of the FISC Rules of Procedure allow for the government or an electronic communication service provider to appeal an order of this Court under §§ 1881a(h)(4) or (5) to the FISC. To date, no electronic communication service provider has opted to challenge a directive issued pursuant to Section 702, although, as noted above, Yahoo refused to comply with government directives issued under the PAA, which resulted in the government invoking a provision under that statute to compel compliance.

As noted above, there have been a number of other instances in which nongovernmental parties have appeared before the Court outside of the context of a direct challenge to a court order or a government directive, particularly recently. Those instances are as follows:

In August 2007, the American Civil Liberties Union (ACLU) filed a motion with the Court for the release of certain records. The Court ordered and received briefing on the matter from the ACLU and the government, and rendered a decision in December 2007. See In re Motion for Release of Court Records, 526 F. Supp. 2d 484 (FISA Ct. 2007).

On May 23, 2013, the Electronic Frontier Foundation (EFF) filed a motion with this Court for consent to disclosure of court records, or in the alternative, a determination of the effect of the Court’s rules on access rights under the Freedom of Information Act. Following briefing by EFF and the government, the Court issued an Opinion and Order on June 12, 2013. All documents filed in this docket are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html under Case No. Misc. 13-01.

On June 12, 2013, the ACLU, the American Civil Liberties Union of the Nation’s Capital, and the Media Freedom and Information Access Clinic (Movants) filed a motion with this Court for the release of Court records. The Court ordered and has received briefing on the matter from the Movants and the government. On July 18, 2013, the Court granted the motions of (1) sixteen members of the House of Representatives and (2) a coalition of news media organizations for leave to file amicus curiae briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html under Case No. Misc. 12-02.

On June 18, 2013, Google, Inc. filed a motion with this Court for declaratory judgment of the company’s first amendment right to publish aggregate information about FISA orders. The
court ordered briefing on the matter. On July 18, 2013, the Court granted the motions of (1) a coalition of news media organizations and (2) the First Amendment Coalition, the ACLU, the Center for Democracy and Technology, the EFF, and TechFreedom for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at [http://www.uscourts.gov/uscourts/courts/fisc/index.html](http://www.uscourts.gov/uscourts/courts/fisc/index.html) under Case No. Misc. 13-03.

On June 19, 2013, Microsoft Corporation filed a motion in this Court for declaratory judgment or other appropriate relief authorizing disclosure of aggregate data regarding any FISA orders it has received. The court ordered briefing on the matter. On July 18, 2013, the Court granted the motions of (1) a coalition of news media organizations and (2) the First Amendment Coalition, the ACLU, the Center for Democracy and Technology, the EFF, and TechFreedom for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at [http://www.uscourts.gov/uscourts/courts/fisc/index.html](http://www.uscourts.gov/uscourts/courts/fisc/index.html) under Case No. Misc. 13-04.

4. *Please describe the process used by the Court to consider and resolve any instances where the government notifies the Court of compliance concerns with any of the FISA authorities.*

Pursuant to 50 U.S.C. § 1803(h), the Court is empowered to ensure compliance with its orders. Additionally, Rule 13(a) of the FISC Rules of Procedure requires the government to file a written notice with the Court immediately upon discovering that any authority or approval granted by the Court has been implemented (either by government officials or others operating pursuant to Court order) in a manner that did not comply with the Court’s authorization or approval or with applicable law. Rule 13(a) also requires the government to notify the Court in writing of the facts and circumstances relevant to the non-compliance; any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

When the government discovers instances of non-compliance, it files notices with the Court as required by Rule 13(a). Because the rule requires the government to “immediately inform the Judge” of a compliance incident, the government typically files a preliminary notice that provides whatever facts are available at the time an incident is discovered. The legal staff review these notices as they are received and call significant matters to the attention of the appropriate judge. In instances in which the non-compliance has not been fully addressed by the time the preliminary Rule 13(a) notice is filed, the Court may seek additional information through telephone calls, meetings, or hearings. Typically, the government will file a final Rule 13(a) notice once the relevant facts are known and any unauthorized collection has been destroyed. However, judges sometimes issue orders directing the government to take specific
Honorable Charles E. Grassley
July 29, 2013
Page 11

actions to address instances of non-compliance either before or after a final notice is
filed, and, less frequently, to cease a course of action that the Court considers non-compliant.
This process is followed for compliance issues in all matters, including matters handled under
Title V and Section 702.

I hope these responses are helpful to the Senate Judiciary Committee in its deliberations.

Sincerely,

Wyatt B. Walton
Presiding Judge

Identical letter sent to: Honorable Patrick J. Leahy
TO THE BENCH, BAR AND PUBLIC:

The attached Rules of Procedure for the Foreign Intelligence Surveillance Court supersede both the February 17, 2006 Rules of Procedure and the May 5, 2006 Procedures for Review of Petitions Filed Pursuant to Section 301(f) of the Foreign Intelligence Surveillance Act of 1978, As Amended. These revised Rules of Procedure are effective immediately.

John D. Bates  
Presiding Judge  
Foreign Intelligence Surveillance Court  

November 1, 2010
# UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT
## Washington, D.C.

## RULES OF PROCEDURE
*Effective November 1, 2010*

<table>
<thead>
<tr>
<th>Rule</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title I. Scope of Rules; Amendment</strong></td>
<td></td>
</tr>
<tr>
<td>1. Scope of Rules</td>
<td>1</td>
</tr>
<tr>
<td>2. Amendment</td>
<td>1</td>
</tr>
<tr>
<td><strong>Title II. National Security Information</strong></td>
<td></td>
</tr>
<tr>
<td>3. National Security Information</td>
<td>1</td>
</tr>
<tr>
<td><strong>Title III. Structure and Powers of the Court</strong></td>
<td></td>
</tr>
<tr>
<td>4. Structure</td>
<td>1</td>
</tr>
<tr>
<td>5. Authority of the Judges</td>
<td>1</td>
</tr>
<tr>
<td><strong>Title IV. Matters Presented to the Court</strong></td>
<td></td>
</tr>
<tr>
<td>6. Means of Requesting Relief from the Court</td>
<td>2</td>
</tr>
<tr>
<td>7. Filing Applications, Certifications, Petitions, Motions, or Other Papers (&quot;Submissions&quot;)</td>
<td>2</td>
</tr>
<tr>
<td>8. Service</td>
<td>3</td>
</tr>
<tr>
<td>9. Time and Manner of Submission of Applications</td>
<td>3</td>
</tr>
<tr>
<td>10. Computation of Time</td>
<td>4</td>
</tr>
<tr>
<td>11. Notice and Briefing of Novel Issues</td>
<td>4</td>
</tr>
<tr>
<td>12. Submission of Targeting and Minimization Procedures</td>
<td>5</td>
</tr>
<tr>
<td>13. Correction of Misstatement or Omission; Disclosure of Non-Compliance</td>
<td>5</td>
</tr>
<tr>
<td>14. Motions to Amend Court Orders</td>
<td>5</td>
</tr>
<tr>
<td>15. Sequestration</td>
<td>5</td>
</tr>
<tr>
<td>16. Returns</td>
<td>6</td>
</tr>
<tr>
<td><strong>Title V. Hearings, Orders, and Enforcement</strong></td>
<td></td>
</tr>
<tr>
<td>17. Hearings</td>
<td>6</td>
</tr>
<tr>
<td>18. Court Orders</td>
<td>6</td>
</tr>
<tr>
<td>19. Enforcement of Orders</td>
<td>7</td>
</tr>
</tbody>
</table>
### Title VI. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1881a(h)

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.</td>
<td>Scope</td>
</tr>
<tr>
<td>21.</td>
<td>Petition to Modify or Set Aside a Directive</td>
</tr>
<tr>
<td>22.</td>
<td>Petition to Compel Compliance With a Directive</td>
</tr>
<tr>
<td>23.</td>
<td>Contents of Petition</td>
</tr>
<tr>
<td>24.</td>
<td>Response</td>
</tr>
<tr>
<td>25.</td>
<td>Length of Petition and Response; Other Papers</td>
</tr>
<tr>
<td>26.</td>
<td>Notification of Presiding Judge</td>
</tr>
<tr>
<td>27.</td>
<td>Assignment</td>
</tr>
<tr>
<td>28.</td>
<td>Review of Petition to Modify or Set Aside a Directive</td>
</tr>
<tr>
<td>29.</td>
<td>Review of Petition to Compel Compliance Pursuant to 50 U.S.C. § 1881a(h)(5)(C)</td>
</tr>
<tr>
<td>30.</td>
<td><em>In Camera</em> Review</td>
</tr>
<tr>
<td>31.</td>
<td>Appeal</td>
</tr>
</tbody>
</table>

### Title VII. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1861(f)

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td>Scope</td>
</tr>
<tr>
<td>33.</td>
<td>Petition Challenging Production or Nondisclosure Order</td>
</tr>
<tr>
<td>34.</td>
<td>Contents of Petition</td>
</tr>
<tr>
<td>35.</td>
<td>Length of Petition</td>
</tr>
<tr>
<td>36.</td>
<td>Request to Stay Production</td>
</tr>
<tr>
<td>37.</td>
<td>Notification of Presiding Judge</td>
</tr>
<tr>
<td>38.</td>
<td>Assignment</td>
</tr>
<tr>
<td>39.</td>
<td>Initial Review</td>
</tr>
<tr>
<td>40.</td>
<td>Response to Petition; Other Papers</td>
</tr>
<tr>
<td>41.</td>
<td>Rulings on Non-frivolous Petitions</td>
</tr>
<tr>
<td>42.</td>
<td>Failure to Comply</td>
</tr>
<tr>
<td>43.</td>
<td><em>In Camera</em> Review</td>
</tr>
<tr>
<td>44.</td>
<td>Appeal</td>
</tr>
</tbody>
</table>

### Title VIII. En Banc Proceedings

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td>Standard for Hearing or Rehearing En Banc</td>
</tr>
<tr>
<td>46.</td>
<td>Initial Hearing En Banc on Request of a Party</td>
</tr>
<tr>
<td>47.</td>
<td>Rehearing En Banc on Petition by a Party</td>
</tr>
<tr>
<td>48.</td>
<td>Circulation of En Banc Petitions and Responses</td>
</tr>
<tr>
<td>49.</td>
<td>Court-Initiated En Banc Proceedings</td>
</tr>
<tr>
<td>50.</td>
<td>Polling</td>
</tr>
<tr>
<td>51.</td>
<td>Stay Pending En Banc Review</td>
</tr>
<tr>
<td>52.</td>
<td>Supplemental Briefing</td>
</tr>
<tr>
<td>53.</td>
<td>Order Granting or Denying En Banc Review</td>
</tr>
</tbody>
</table>
Title IX. Appeals

54. How Taken ....................................................... 14
55. When Taken ....................................................... 14
56. Stay Pending Appeal ............................................. 14
57. Motion to Transmit the Record .................................. 14
58. Transmitting the Record ........................................ 14
59. Oral Notification to the Court of Review ....................... 14

Title X. Administrative Provisions

60. Duties of the Clerk ............................................... 14
61. Office Hours ...................................................... 15
62. Release of Court Records ....................................... 15
63. Practice Before Court .......................................... 15
Title I. Scope of Rules; Amendment

Rule 1. Scope of Rules. These rules, which are promulgated pursuant to 50 U.S.C. § 1803(g), govern all proceedings in the Foreign Intelligence Surveillance Court ("the Court"). Issues not addressed in these rules or the Foreign Intelligence Surveillance Act, as amended ("the Act"), may be resolved under the Federal Rules of Criminal Procedure or the Federal Rules of Civil Procedure.

Rule 2. Amendment. Any amendment to these rules must be promulgated in accordance with 28 U.S.C. § 2071.

Title II. National Security Information

Rule 3. National Security Information. In all matters, the Court and its staff shall comply with the security measures established pursuant to 50 U.S.C. §§ 1803(c), 1822(e), 1861(y)(4), and 1881a(k)(1), as well as Executive Order 13526, "Classified National Security Information" (or its successor). Each member of the Court's staff must possess security clearances at a level commensurate to the individual's responsibilities.

Title III. Structure and Powers of the Court

(a) Composition. In accordance with 50 U.S.C. § 1803(a), the Court consists of United States District Court Judges appointed by the Chief Justice of the United States.
(b) Presiding Judge. The Chief Justice designates the "Presiding Judge."

Rule 5. Authority of the Judges.
(a) Scope of Authority. Each Judge may exercise the authority vested by the Act and such other authority as is consistent with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.
(b) Referring Matters to Other Judges. Except for matters involving a denial of an application for an order, a Judge may refer any matter to another Judge of the Court with that Judge's consent. If a Judge directs the government to supplement an application, the Judge may direct the government to present the renewal of that application to the same Judge. If a matter is presented to a Judge who is unavailable or whose tenure on the Court expires while the matter is pending, the Presiding Judge may re-assign the matter.
(c) Supplementation. The Judge before whom a matter is pending may order a party to furnish any information that the Judge deems necessary.
Title IV. Matters Presented to the Court

Rule 6. Means of Requesting Relief from the Court.
(a) Application. The government may, in accordance with 50 U.S.C. §§ 1804, 1823, 1842, 1851, 1881(b)(b), 1881c(b), or 1881d(a), file an application for a Court order ("application").
(b) Certification. The government may, in accordance with 50 U.S.C. § 1881a(g), file a certification concerning the targeting of non-United States persons reasonably believed to be located outside the United States ("certification").
(c) Petition. A party may, in accordance with 50 U.S.C. §§ 1861(f) and 1881a(h) and the Supplemental Procedures in Titles VI and VII of these Rules, file a petition for review of a production or nondisclosure order issued under 50 U.S.C. § 1861 or for review or enforcement of a directive issued under 50 U.S.C. § 1881a ("petition").
(d) Motion. A party seeking relief, other than pursuant to an application, certification, or petition permitted under the Act and these Rules, must do so by motion ("motion").

Rule 7. Filing Applications, Certifications, Petitions, Motions, or Other Papers ("Submissions").
(a) Filing. A submission is filed by delivering it to the Clerk or as otherwise directed by the Clerk in accordance with Rule 7(k).
(b) Original and One Copy. Except as otherwise provided, a signed original and one copy must be filed with the Clerk.
(c) Form. Unless otherwise ordered, all submissions must be:
(1) on 8½-by-11-inch opaque white paper, and
(2) typed (double-spaced) or reproduced in a manner that produces a clear black image.
(d) Electronic Filing. The Clerk, when authorized by the Court, may accept and file submissions by any reliable, and appropriately secure, electronic means.
(e) Facsimile or Scanned Signature. The Clerk may accept for filing a submission bearing a facsimile or scanned signature in lieu of the original signature. Upon acceptance, a submission bearing a facsimile or scanned signature is the original Court record.
(f) Citations. Each submission must contain citations to pertinent provisions of the Act.
(g) Contents. Each application and certification filed by the government must be approved and certified in accordance with the Act, and must contain the statements and other information required by the Act.

(h) Contact Information in Adversarial Proceedings.
(1) Filing by a Party Other Than the Government. A party other than the government must include in the initial submission the party's full name, address, and telephone number, or, if the party is represented by counsel, the full name of the party and the party's counsel, as well as counsel's address, telephone number, facsimile number, and bar membership information.
(2) Filing by the Government. In an adversarial proceeding, the initial
submission filed by the government must include the full names of the attorneys representing the United States and their mailing addresses, telephone numbers, and facsimile numbers.

(i) Information Concerning Security Clearances in Adversarial Proceedings. A party other than the government must:

1. state in the initial submission whether the party (or the party's responsible officers or employees) and counsel for the party hold security clearances;
2. describe the circumstances in which such clearances were granted; and
3. identify the federal agencies granting the clearances and the classification levels and compartments involved.

(j) Ex Parte Review. At the request of the government in an adversarial proceeding, the Judge must review ex parte and in camera any submissions by the government, or portions thereof, which may include classified information. Except as otherwise ordered, if the government files ex parte a submission that contains classified information, the government must file and serve on the non-governmental party an unclassified or redacted version. The unclassified or redacted version, at a minimum, must clearly articulate the government's legal arguments.

(k) Instructions for Delivery to the Court. A party may obtain instructions for making submissions permitted under the Act and these Rules by contacting the Clerk at (202) 357-6250.

Rule 8. Service.

(a) By a Party Other than the Government. A party other than the government must, at or before the time of filing a submission permitted under the Act and these Rules, serve a copy on the government. Instructions for effecting service must be obtained by contacting the Security and Emergency Planning Staff, United States Department of Justice, by telephone at (202) 514-2094.

(b) By the Government. At or before the time of filing a submission in an adversarial proceeding, the government must, subject to Rule 7(j), serve a copy by hand delivery or by overnight delivery or by counsel for the other party, or, if the party is not represented by counsel, on the party directly.

(c) Certificate of Service. A party must include a certificate of service specifying the time and manner of service.


(a) Proposed Applications. Except when an application is being submitted following an emergency authorization pursuant to 50 U.S.C. §§ 1805(e), 1824(e), 1843, 1881b(d), or 1881c(d) ("emergency authorization"), or as otherwise permitted by the Court, proposed applications must be submitted by the government no later than seven days before the government seeks to have the matter entertained by the Court. Proposed applications submitted following an emergency authorization must be submitted as soon after such authorization as is reasonably practicable.

(b) Final Applications. Unless the Court permits otherwise, the final application,
including all signatures, approvals, and certifications required by the Act, must be filed
no later than 10:00 a.m. Eastern Time on the day the government seeks to have the matter
entertained by the Court.
(c) Proposed Orders. Each proposed application and final application submitted to the
Court must include any pertinent proposed orders.
(d) Number of Copies. Notwithstanding Rule 7(b), unless the Court directs otherwise,
only one copy of a proposed application must be submitted and only the original final
application must be filed.
(e) Notice of Changes. No later than the time the final application is filed, the
government must identify any differences between the final application and the proposed
application.

Rule 10. Computation of Time. The following rules apply in computing a time period
specified by these Rules or by Court order:
(a) Day of the Event Excluded. Exclude the day of the event that triggers the period.
(b) Compute Time Using Calendar Days. Compute time using calendar days, not
business days.
(c) Include the Last Day. Include the last day of the period; but if the last day is a
Saturday, Sunday, or legal holiday, the period continues to run until the next day that is
not a Saturday, Sunday, or legal holiday.

(a) Notice to the Court. If a submission by the government for Court action involves an
issue not previously presented to the Court — including, but not limited to, a novel issue
of technology or law — the government must inform the Court in writing of the nature
and significance of that issue.
(b) Submission Relating to New Techniques. Prior to requesting authorization to use a
new surveillance or search technique, the government must submit a memorandum to the
Court that:
   (1) explains the technique;
   (2) describes the circumstances of the likely implementation of the technique;
   (3) discusses any legal issues apparently raised; and
   (4) describes the proposed minimization procedures to be applied.
At the latest, the memorandum must be submitted as part of the first proposed application
or other submission that seeks to employ the new technique.
(c) Novel Implementation. When requesting authorization to use an existing surveillance
or search technique in a novel context, the government must identify and address any new
minimization or other issues in a written submission made, at the latest, as part of the
application or other filing seeking such authorization.
(d) Legal Memorandum. If an application or other request for action raises an issue of
law not previously considered by the Court, the government must file a memorandum of
law in support of its position on each new issue. At the latest, the memorandum must be
submitted as part of the first proposed application or other submission that raises the issue.

Rule 12. Submission of Targeting and Minimization Procedures. In a matter involving Court review of targeting or minimization procedures, such procedures may be set out in full in the government's submission or may be incorporated by reference to procedures approved in a prior docket. Procedures that are incorporated by reference to a prior docket may be supplemented, but not otherwise modified, in the government's submission. Otherwise, proposed procedures must be set forth in a clear and self-contained manner, without resort to cross-referencing.

Rule 13. Correction of Misstatement or Omission; Disclosure of Non-Compliance.
(a) Correction of Material Facts. If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government, in writing, must immediately inform the Judge to whom the submission was made of:
(1) the misstatement or omission;
(2) any necessary correction;
(3) the facts and circumstances relevant to the misstatement or omission;
(4) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
(5) how the government proposes to dispose of or treat any information obtained as a result of the misstatement or omission.
(b) Disclosure of Non-Compliance. If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government, in writing, must immediately inform the Judge to whom the submission was made of:
(1) the non-compliance;
(2) the facts and circumstances relevant to the non-compliance;
(3) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
(4) how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

Rule 14. Motions to Amend Court Orders. Unless the Judge who issued the order granting an application directs otherwise, a motion to amend the order may be presented to any other Judge.

Rule 15. Sequestration. Except as required by Court-approved minimization procedures, the government must not submit material for sequestration with the Court without the prior approval of the Presiding Judge. To obtain such approval, the government must, prior to tendering the material to the Court for sequestration, file a motion stating the circumstances of the material's acquisition and explaining why it is necessary for such material to be retained in the custody of the Court.

(a) Time for Filing.
   (1) Search Orders. Unless the Court directs otherwise, a return must be made and filed either at the time of submission of a proposed renewal application or within 90 days of the execution of a search order, whichever is sooner.
   (2) Other Orders. The Court may direct the filing of other returns at a time and in a manner that it deems appropriate.

(b) Contents. The return must:
   (1) notify the Court of the execution of the order;
   (2) describe the circumstances and results of the search or other activity including, where appropriate, an inventory;
   (3) certify that the execution was in conformity with the order or describe and explain any deviation from the order; and
   (4) include any other information as the Court may direct.

Title V. Hearings, Orders, and Enforcement

Rule 17. Hearings.

(a) Scheduling. The Judge to whom a matter is presented or assigned must determine whether a hearing is necessary and, if so, set the time and place of the hearing.

(b) Ex Parte. Except as the Court otherwise directs or the Rules otherwise provide, a hearing in a non-adversarial matter must be ex parte and conducted within the Court’s secure facility.

(c) Appearances. Unless excused, the government official providing the factual information in an application or certification and an attorney for the applicant must attend the hearing, along with other representatives of the government, and any other party, as the Court may direct or permit.

(d) Testimony; Oath; Recording of Proceedings. A Judge may take testimony under oath and receive other evidence. The testimony may be recorded electronically or as the Judge may otherwise direct, consistent with the security measures referenced in Rule 3.

Rule 18. Court Orders.

(a) Citations. All orders must contain citations to pertinent provisions of the Act.

(b) Denying Applications.
   (1) Written Statement of Reasons. If a Judge denies the government’s application, the Judge must immediately provide a written statement of each reason for the decision and cause a copy of the statement to be served on the government.
   (2) Previously Denied Application. If a Judge denies an application or other request for relief by the government, any subsequent submission on the matter must be referred to that Judge.
(c) Expiration Dates. An expiration date in an order must be stated using Eastern Time and must be computed from the date and time of the Court's issuance of the order, or, if applicable, of an emergency authorization.

(d) Electronic Signatures. The Judge may sign an order by any reliable, appropriately secure electronic means, including facsimile.


(a) Show Cause Motions. If a person or entity served with a Court order (the "recipient") fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly. The motion must be presented to the Judge who entered the underlying order.

(b) Proceedings.

(1) An order to show cause must:
   (i) confirm that the underlying order was issued;
   (ii) schedule further proceedings; and
   (iii) afford the recipient an opportunity to show cause why the recipient should not be held in contempt.

(2) A Judge must conduct any proceeding on a motion to show cause in camera. The Clerk must maintain all records of the proceedings in conformance with 50 U.S.C. § 1803(c).

(3) If the recipient fails to show cause for noncompliance with the underlying order, the Court may find the recipient in contempt and enter any order it deems necessary and appropriate to compel compliance and to sanction the recipient for noncompliance with the underlying order.

(4) If the recipient shows cause for noncompliance or if the Court concludes that the order should not be enforced as issued, the Court may enter any order it deems appropriate.

Title VI. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1881a(b)

Rule 20. Scope. Together with the generally-applicable provisions of these Rules concerning filing, service, and other matters, these supplemental procedures apply in proceedings under 50 U.S.C. § 1881a(b).

Rule 21. Petition to Modify or Set Aside a Directive. An electronic communication service provider ("provider"), who receives a directive issued under 50 U.S.C. § 1881a(b)(1), may file a petition to modify or set aside such directive under 50 U.S.C. § 1881a(b)(4). A petition may be filed by the provider's counsel.
Rule 22. Petition to Compel Compliance With a Directive. In the event a provider fails to comply with a directive issued under 50 U.S.C. § 1881a(h)(1), the government may, pursuant to 50 U.S.C. § 1881a(h)(5), file a petition to compel compliance with the directive.

Rule 23. Contents of Petition. The petition must:
(a) state clearly the relief being sought;
(b) state concisely the factual and legal grounds for modifying, setting aside, or compelling compliance with the directive at issue;
(c) include a copy of the directive and state the date on which the directive was served on the provider; and
(d) state whether a hearing is requested.

(a) By Government. The government may, within seven days following notification under Rule 28(b) that plenary review is necessary, file a response to a provider’s petition.
(b) By Provider. The provider may, within seven days after service of a petition by the government to compel compliance, file a response to the petition.

Rule 25. Length of Petition and Response; Other Papers.
(a) Length. Unless the Court directs otherwise, a petition and response each must not exceed 20 pages in length, including any attachments (other than a copy of the directive at issue).
(b) Other papers. No supplements, replies, or sur-replies may be filed without leave of the Court.

Rule 26. Notification of Presiding Judge. Upon receipt, the Clerk must notify the Presiding Judge that a petition to modify, set aside, or compel compliance with a directive issued under 50 U.S.C. § 1881a(h)(1) has been filed. If the Presiding Judge is not reasonably available when the Clerk receives a petition, the Clerk must notify each of the local Judges, in order of seniority on the Court, and, if necessary, each of the other Judges, in order of seniority on the Court, until a Judge who is reasonably available has received notification. The reasonably available Judge who receives notification will be the acting Presiding Judge ("Presiding Judge") for the case.

Rule 27. Assignment.
(a) Presiding Judge. As soon as possible after receiving notification from the Clerk that a petition has been filed, and no later than 24 hours after the filing of the petition, the Presiding Judge must assign the matter to a Judge in the petition review pool established by 50 U.S.C. § 1803(e)(1). The Clerk must record the date and time of the assignment.
(b) Transmitting Petition. The Clerk must transmit the petition to the assigned Judge as soon as possible but no later than 24 hours after being notified of the assignment by the Presiding Judge.

(a) Initial Review Pursuant to 50 U.S.C. § 1881a(h)(4)(D).

(1) A Judge must conduct an initial review of a petition to modify or set aside a directive within five days after being assigned such petition.

(2) If the Judge determines that the provider’s claims, defenses, or other legal contentions are not warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the Judge must promptly deny such petition, affirm the directive, and order the provider to comply with the directive. Upon making such determination or promptly thereafter, the Judge must provide a written statement of reasons. The Clerk must transmit the ruling and statement of reasons to the provider and the government.


(1) If the Judge determines that the petition requires plenary review, the Court must promptly notify the parties. The Judge must provide a written statement of reasons for the determination.

(2) The Judge must affirm, modify, or set aside the directive that is the subject of the petition within the time permitted under 50 U.S.C. §§ 1881a(h)(4)(E) and 1881a(j)(2).

(3) The Judge may hold a hearing or conduct proceedings solely on the papers filed by the provider and the government.

(c) Burden. Pursuant to 50 U.S.C. § 1881a(h)(4)(C), a Judge may grant the petition only if the Judge finds that the challenged directive does not meet the requirements of 50 U.S.C. § 1881a or is otherwise unlawful.

(d) Continued Effect. Pursuant to 50 U.S.C. § 1881a(h)(4)(F), any directive not explicitly modified or set aside by the Judge remains in full effect.


(a) The Judge reviewing the government’s petition to compel compliance with a directive must, within the time permitted under 50 U.S.C. §§ 1881a(h)(5)(C) and 1881a(j)(2), issue an order requiring the provider to comply with the directive or any part of it, as issued or as modified, if the Judge finds that the directive meets the requirements of 50 U.S.C. § 1881a and is otherwise lawful.

(b) The Judge must provide a written statement of reasons for the determination. The Clerk must transmit the ruling and statement of reasons to the provider and the government.

Rule 30. In Camera Review. Pursuant to 50 U.S.C. § 1803(e)(2), the Court must review a petition under 50 U.S.C. § 1881a(h) and conduct related proceedings in camera.

Rule 31. Appeal. Pursuant to 50 U.S.C. § 1881a(h)(6) and subject to Rules 54 through 59 of these Rules, the government or the provider may petition the Foreign Intelligence Surveillance Court of Review (“Court of Review”) to review the Judge’s ruling.
Title VII. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1861(f)

Rule 32. Scope. Together with the generally-applicable provisions of these Rules regarding filing, service, and other matters, these supplemental procedures apply in proceedings under 50 U.S.C. § 1861(f).

Rule 33. Petition Challenging Production or Nondisclosure Order.
(a) Who May File. The recipient of a production order or nondisclosure order under 50 U.S.C. § 1861 ("petitioner") may file a petition challenging the order pursuant to 50 U.S.C. § 1861(f). A petition may be filed by the petitioner's counsel.
(b) Time to File Petition.
(1) Challenging a Production Order. The petitioner must file a petition challenging a production order within 20 days after the order has been served.
(2) Challenging a Nondisclosure Order. A petitioner may not file a petition challenging a nondisclosure order issued under 50 U.S.C. § 1861(d) earlier than one year after the order was entered.
(3) Subsequent Petition Challenging a Nondisclosure Order. If a Judge denies a petition to modify or set aside a nondisclosure order, the petitioner may not file a subsequent petition challenging the same nondisclosure order earlier than one year after the date of the denial.

Rule 34. Contents of Petition. A petition must:
(a) state clearly the relief being sought;
(b) state concisely the factual and legal grounds for modifying or setting aside the challenged order;
(c) include a copy of the challenged order and state the date on which it was served on the petitioner; and
(d) state whether a hearing is requested.

Rule 35. Length of Petition. Unless the Court directs otherwise, a petition may not exceed 20 pages in length, including any attachments (other than a copy of the challenged order).

Rule 36. Request to Stay Production.
(a) Petition Does Not Automatically Effect a Stay. A petition does not automatically stay the underlying order. A production order will be stayed only if the petitioner requests a stay and the Judge grants such relief.
(b) Stay May Be Requested Prior to Filing of a Petition. A petitioner may request the Court to stay the production order before filing a petition challenging the order.

Rule 37. Notification of Presiding Judge. Upon receipt, the Clerk must notify the Presiding Judge that a petition challenging a production or nondisclosure order has been filed. If the Presiding Judge is not reasonably available when the Clerk receives the petition, the Clerk must
notify each of the local Judges, in order of seniority on the Court, and, if necessary, each of the
other Judges, in order of seniority on the Court, until a Judge who is reasonably available has
received notification. The reasonably available Judge who receives notification will be the acting
Presiding Judge ("Presiding Judge") for the case.

Rule 38. Assignment.
(a) Presiding Judge. Immediately after receiving notification from the Clerk that a petition has been filed, the Presiding Judge must assign the matter to a Judge in the petition pool established by 50 U.S.C. § 1803(c)(1). The Clerk must record the date and
time of the assignment.
(b) Transmitting Petition. The Clerk must transmit the petition to the assigned Judge as soon as possible but no later than 24 hours after being notified of the assignment by the
Presiding Judge.

Rule 39. Initial Review.
(a) When. The Judge must review the petition within 72 hours after being assigned the petition.
(b) Frivolous Petition. If the Judge determines that the petition is frivolous, the Judge must:
   (1) immediately deny the petition and affirm the challenged order;
   (2) promptly provide a written statement of the reasons for the denial; and
   (3) provide a written ruling, together with the statement of reasons, to the Clerk, who must transmit the ruling and statement of reasons to the petitioner and the government.
(c) Non-Frivolous Petition.
   (1) Scheduling. If the Judge determines that the petition is not frivolous, the Judge must promptly issue an order that sets a schedule for its consideration. The Clerk must transmit the order to the petitioner and the government.
   (2) Manner of Proceeding. The judge may hold a hearing or conduct the proceedings solely on the papers filed by the petitioner and the government.

Rule 40. Response to Petition; Other Papers.
(a) Government's Response. Unless the Judge orders otherwise, the government must file a response within 20 days after the issuance of the initial scheduling order pursuant to
Rule 39(c). The response must not exceed 20 pages in length, including any attachments
(other than a copy of the challenged order).
(b) Other Papers. No supplements, replies, or sur-replies may be filed without leave of the Court.

Rule 41. Rulings on Non-frivolous Petitions.
(a) Written Statement of Reasons. If the Judge determines that the petition is not frivolous, the Judge must promptly provide a written statement of the reasons for modifying, setting aside, or affirming the production or nondisclosure order.
(b) Affirming the Order. If the Judge does not modify or set aside the production or nondisclosure order, the Judge must affirm it and order the recipient promptly to comply with it.

(c) Transmitting the Judge's Ruling. The Clerk must transmit the Judge's ruling and written statement of reasons to the petitioner and the government.

Rule 42. Failure to Comply. If a recipient fails to comply with an order affirmed under 50 U.S.C. § 1861(f), the government may file a motion seeking immediate enforcement of the affirmed order. The Court may consider the government's motion without receiving additional submissions or convening further proceedings on the matter.

Rule 43. In Camera Review. Pursuant to 50 U.S.C. § 1803(e)(2), the Court must review a petition under 50 U.S.C. § 1861(f) and conduct related proceedings in camera.

Rule 44. Appeal. Pursuant to 50 U.S.C. § 1861(f)(3) and subject to Rules 54 through 59 of these Rules, the government or the petitioner may petition the Court of Review to review the Judge's ruling.

Title VIII. En Banc Proceedings

Rule 45. Standard for Hearing or Rehearing En Banc. Pursuant to 50 U.S.C. § 1803(a)(2)(A), the Court may order a hearing or rehearing en banc only if it is necessary to secure or maintain uniformity of the Court's decisions, or the proceeding involves a question of exceptional importance.

Rule 46. Initial Hearing En Banc on Request of a Party. The government in any proceeding, or a party in a proceeding under 50 U.S.C. § 1861(f) or 50 U.S.C. § 1881a(h)(4)-(5), may request that the matter be entertained from the outset by the full Court. However, initial hearings en banc are extraordinary and will be ordered only when a majority of the Judges determines that a matter is of such immediate and extraordinary importance that initial consideration by the en banc Court is necessary, and en banc review is feasible in light of applicable time constraints on Court action.

Rule 47. Rehearing En Banc on Petition by a Party.

(a) Timing of Petition and Response. A party may file a petition for rehearing en banc permitted under 50 U.S.C. § 1803(a)(2) no later than 30 days after the challenged order or decision is entered. In an adversarial proceeding in which a petition for rehearing en banc is permitted under § 1803(a)(2), a party must file a response to the petition within 14 days after filing and service of the petition.

(b) Length of Petition and Response. Unless the Court directs otherwise, a petition for rehearing en banc and a response to a petition for rehearing en banc each must not exceed 15 pages, including any attachments (other than the challenged order or decision).
Rule 48. Circulation of En Banc Petitions and Responses. The Clerk must, after consulting with the Presiding Judge and in a manner consistent with applicable security requirements, promptly provide a copy of any timely-filed en banc petition permitted under 50 U.S.C. § 1803(a)(2), and any timely-filed response thereto, to each Judge.

Rule 49. Court-Initiated En Banc Proceedings. A Judge to whom a matter has been presented may request that all Judges be polled with respect to whether the matter should be considered or reconsidered en banc. On a Judge's request, the Clerk must, after consulting with the Presiding Judge and in a manner consistent with applicable security requirements, promptly provide notice of the request, along with a copy of pertinent materials, to every Judge.

Rule 50. Polling.
   (a) Deadline for Vote. The Presiding Judge must set a deadline for the Judges to submit their vote to the Clerk on whether to grant a hearing or rehearing en banc. The deadline must be communicated to all Judges at the time the petition or polling request is circulated.
   (b) Vote on Stay. In the case of rehearing en banc, the Presiding Judge may request that all Judges also vote on whether and to what extent the challenged order or ruling should be stayed or remain in effect if rehearing en banc is granted, pending a decision by the en banc Court on the merits.

Rule 51. Stay Pending En Banc Review.
   (a) Stay or Modifying Order. In accordance with 50 U.S.C. §§ 1803(a)(2)(B) and 1803(f), the Court en banc may enter a stay or modifying order while en banc proceedings are pending.
   (b) Statement of Position Regarding Continued Effect of Challenged Order. A petition for rehearing en banc and any response to the petition each must include a statement of the party's position as to whether and to what extent the challenged order should remain in effect if rehearing en banc is granted, pending a decision by the en banc Court on the merits.

Rule 52. Supplemental Briefing. Upon ordering hearing or rehearing en banc, the Court may require the submission of supplemental briefs.

Rule 53. Order Granting or Denying En Banc Review.
   (a) Entry of Order. If a majority of the Judges votes within the time allotted for polling that a matter be considered en banc, the Presiding Judge must direct the Clerk to enter an order granting en banc review. If a majority of the Judges does not vote to grant hearing or rehearing en banc within the time allotted for polling, the Presiding Judge must direct the Clerk to enter an order denying en banc review.
   (b) Other Issues. The Presiding Judge may set the time of an en banc hearing and the time and scope of any supplemental hearing in the order granting en banc review. The
order may also address whether and to what extent the challenged order or ruling will be stayed or remain in effect pending a decision by the en banc Court on the merits.

Title IX. Appeals

Rule 54. How Taken. An appeal to the Court of Review, as permitted by law, may be taken by filing a petition for review with the Clerk.

Rule 55. When Taken.
(a) Generally. Except as the Act provides otherwise, a party must file a petition for review no later than 30 days after entry of the decision or order as to which review is sought.
(b) Effect of En Banc Proceedings. Following the timely submission of a petition for rehearing en banc permitted under 50 U.S.C. § 1803(a)(2) or the grant of rehearing en banc on the Court's own initiative, the time otherwise allowed for taking an appeal runs from the date on which such petition is denied or dismissed or, if en banc review is granted, from the date of the decision of the en banc Court on the merits.

Rule 56. Stay Pending Appeal. In accordance with 50 U.S.C. § 1803(f), the Court may enter a stay of an order or an order modifying an order while an appeal is pending.

Rule 57. Motion to Transmit the Record. Together with the petition for review, the party filing the appeal must also file a motion to transmit the record to the Court of Review.

Rule 58. Transmitting the Record. The Clerk must arrange to transmit the record under seal to the Court of Review as expeditiously as possible, no later than 30 days after an appeal has been filed. The Clerk must include a copy of the Court's statement of reasons for the decision or order appealed from as part of the record on appeal.

Rule 59. Oral Notification to the Court of Review. The Clerk must orally notify the Presiding Judge of the Court of Review promptly upon the filing of a petition for review.

Title X. Administrative Provisions

Rule 60. Duties of the Clerk.
(a) General Duties. The Clerk supports the work of the Court consistent with the directives of the Presiding Judge. The Presiding Judge may authorize the Clerk to delegate duties to staff in the Clerk's office or other designated individuals.
(b) Maintenance of Court Records. The Clerk:
(1) maintains the Court's docket and records — including records and recordings of proceedings before the Court — and the seal of the Court;
(2) accepts papers for filing;
(3) keeps all records, pleadings, and files in a secure location, making those materials available only to persons authorized to have access to them; and
(4) performs any other duties, consistent with the usual powers of a Clerk of Court, as the Presiding Judge may authorize.

Rule 61. Office Hours. Although the Court is always open, the regular business hours of the Clerk's Office are 9:00 a.m. to 5:00 p.m. daily except Saturdays, Sundays, and legal holidays. Except when the government submits an application following an emergency authorization, or when the Court otherwise directs, any filing outside these hours will be recorded as received at the start of the next business day.

(a) Publication of Opinions. The Judge who authored an order, opinion, or other decision may sua sponte or on motion by a party request that it be published. Upon such request, the Presiding Judge, after consulting with other Judges of the Court, may direct that an order, opinion or other decision be published. Before publication, the Court may, as appropriate, direct the Executive Branch to review the order, opinion, or other decision and redact it as necessary to ensure that properly classified information is appropriately protected pursuant to Executive Order 13526 (or its successor).
(b) Other Records. Except when an order, opinion, or other decision is published or provided to a party upon issuance, the Clerk may not release it, or other related record, without a Court order. Such records must be released in conformance with the security measures referenced in Rule 3.
(c) Provision of Court Records to Congress.
   (1) By the Government. The government may provide copies of Court orders, opinions, decisions, or other Court records, to Congress, pursuant to 50 U.S.C. §§ 1871(a)(2), 1871(c), or 1881(b)(1)(D), or any other statutory requirement, without prior motion to and order by the Court. The government, however, must contemporaneously notify the Court in writing whenever it provides copies of Court records to Congress and must include in the notice a list of the documents provided.
   (2) By the Court. The Presiding Judge may provide copies of Court orders, opinions, decisions, or other Court records to Congress. Such disclosures must be made in conformance with the security measures referenced in Rule 3.

Rule 63. Practice Before Court. An attorney may appear on a matter with the permission of the Judge before whom the matter is pending. An attorney who appears before the Court must be a licensed attorney and a member, in good standing, of the bar of a United States district or circuit court, except that an attorney who is employed by and represents the United States or any of its agencies in a matter before the Court may appear before the Court regardless of federal bar membership. All attorneys appearing before the Court must have the appropriate security clearance.
March 27, 2013

Honorable Dianne Feinstein
United States Senate
Washington, DC 20510

Dear Senator Feinstein:

I am writing in response to your letter dated February 13, 2013, addressed to then-Presiding Judge John D. Bates, in which you requested that the Foreign Intelligence Surveillance Court (FISC) consider providing written summaries of its significant opinions in a manner that permits declassification by separating the classified facts from the legal analysis. I share your view that the FISC plays a crucial role in construing the Foreign Intelligence Surveillance Act (FISA), and believe that it is essential that Congress be kept informed of significant opinions of the FISC that interpret the FISA provisions.

I understand that the Executive Branch provides the Intelligence and Judiciary Committees with all significant FISC opinions, albeit in classified form. I also recognize the potential benefit of better informing the public about how the FISC applies and interprets FISA — for example, by enhancing public participation in congressional deliberations. There are, however, serious obstacles that must be considered regarding your request for summaries of FISC opinions.

In some circumstances, a federal court through its staff may prepare a summary of an opinion for the convenience of the public, such as a syllabus that accompanies a Supreme Court opinion. But where this practice is common, the full opinion is made equally available as well. The summary is merely a guide to the full opinion, not a means of disclosing some parts of that opinion while concealing other parts. If a summary is to be offered as a substitute for the full opinion, then several special concerns arise. Summarizing a judicial opinion of any length or complexity entails losing more nuanced or technical points of a court’s analysis. This loss does not involve a serious risk of confusing or misleading a reader if the full opinion is also available. Without the full opinion, however, the summary is much more likely to result in misunderstanding or confusion regarding the court’s decision or reasoning.
Honorables Dianne Feinstein
Page 2

For FISC opinions specifically, there is also the very real problem of separating the classified facts from the legal analysis. While classification determinations are made by the Executive Branch in the first instance, the facts presented in applications to the FISC always or almost always involve classified intelligence activities, the disclosure of which could be harmful to the nation’s security. As members of Congress who have seen the opinions know, most FISC opinions rest heavily on the facts presented in the particular matter before the court. Thus, in most cases, the facts and the legal analysis are so inextricably intertwined that excising the classified information from the FISC’s analysis would result in a remnant void of much or any useful meaning. Consequently, the summaries you request are unlikely, as a general matter, to serve the purpose of meaningfully informing the public about the FISC’s determinations.

Your request that the FISC prepare summaries of significant interpretations of the law would present additional concerns for previously issued opinions. Article III courts cannot issue advisory opinions. For a court to revisit and reformulate its prior reasoning outside the context of a matter actively before the court may implicate that prohibition. There are also practical considerations with a post hoc summary. For example, if the original opinion had been issued by a judge who is no longer serving on the FISC, another judge would be responsible for preparing the interpretive summary. Insofar as different judges may view particular points of the analysis as more or less important to an opinion as a whole, the summary may be an amalgam of the views of the issuing judge and the summarizing judge. Such procedural complications may lead to further confusion and distortion in the summaries, and imply a lack of finality to FISC opinions. Finally, there are resource considerations. The small number of judges, attorneys, and staff that comprise the FISC are fully occupied by its current caseload. Given the difficulties noted above, the effort to draft summaries of previously issued opinions would have a detrimental impact on the FISC’s ability to address matters currently before the court.

 Rather than summaries, in a few exceptional cases FISC opinions that have contained no classified information, or a small amount of readily excisable classified information, have been made available to the public. Those matters involved the rare circumstance where a FISC decision relied either solely on an interpretation of law or where the classified facts were not inextricably intertwined with the court’s analysis, so that the FISC was able to make its decisions publically available. In fact, the FISC’s Rules of Procedure provide a mechanism for a judge to request the publication of an order, opinion, or other decision. See FISC Rule 62(a). This procedure, where appropriate, contemplates a review by the Executive Branch for the redaction of classified information. Indeed, as you mention, the Executive Branch has indicated that it will seek to provide declassified opinions to the extent it may become feasible to do so.
Recognizing the importance of this issue and your concerns, I have provided a copy of your letter to all of the current judges of the FISC, as well as the Foreign Intelligence Surveillance Court of Review (FISCR), and will ensure that any new judges appointed to the FISC also receive a copy of your letter. In addition, at the FISC’s upcoming semi-annual meeting in May, I will ensure that all of the judges are aware of the procedures that are available under Rule 62.(a) and encourage them to avail themselves of these procedures when appropriate. I will also encourage them to consider structuring opinions to facilitate declassification, if they believe doing so is warranted in a particular case. Realistically, however, I would not anticipate many such cases given the fact-intensive nature of FISC opinions, as described above. Of course, the FISC is also prepared to carry out its responsibilities with respect to the review process currently underway by the Executive Branch that has been detailed to you in previous correspondence.

Sincerely,

[Signature]

Reggie B. Walton
Presiding Judge, U.S. Foreign Intelligence Surveillance Court

cc: Honorable Morris S. Arnold
Presiding Judge, U.S. Foreign Intelligence Surveillance Court of Review

The Honorable James Clapper
Director of National Intelligence

The Honorable Eric H. Holder, Jr.
Attorney General

Identical letter sent to: Honorable Ron Wyden
Honorable Mark Udall
Honorable Jeff Merkley
JOINT STATEMENT FOR THE RECORD
OF

JAMES R. CLAPPER
DIRECTOR OF NATIONAL INTELLIGENCE

GENERAL KEITH B. ALEXANDER
DIRECTOR
NATIONAL SECURITY AGENCY
CHIEF
CENTRAL SECURITY SERVICE

BEFORE THE
SENATE COMMITTEE ON THE JUDICIARY

OCTOBER 2, 2013
Joint Statement for the Record of

James R. Clapper
Director of National Intelligence

General Keith B. Alexander
Director, National Security Agency and Chief, Central Security Service

Before the
Senate Committee on the Judiciary

October 2, 2013

Thank you for inviting us to discuss the Administration’s efforts to enhance public confidence in the important intelligence collection programs that have been the subject of unauthorized disclosures since earlier this year: the collection of bulk telephony metadata under the business records provision found in section 215 of the USA PATRIOT Act, and the targeting of non-U.S. persons overseas under section 702 of FISA. We remain committed, as we review these activities, both to ensuring that we have the authorities we need to collect important foreign intelligence to protect the country from terrorism and other threats to national security, and to protecting privacy and civil liberties in a manner consistent with our values. We also remain committed to working closely with this Committee as any modifications to these activities are considered. We understand that some of the initiatives announced by the President in his
statement on August 9 are of interest to the Committee, and we welcome the opportunity to
discuss them with you and to work together in moving forward.

The first step in promoting greater public confidence in these intelligence activities is to
provide greater transparency so that the American people understand what the activities are, how
they function, and how they are overseen. As you know, many of the reports appearing in the
media concerning the scope of the Government’s intelligence collection efforts have been
inaccurate, including with respect to the collection carried out under sections 215 and 702. In
response, the Administration has released substantial information since June to increase
transparency and public understanding, while also working to ensure that these releases are
consistent with national security.

We have worked to provide the public greater insight into the operation of the bulk
telephony metadata business records collection program under section 215. In early June, the
Director of National Intelligence (DNI) released a public statement explaining that the program
is carried out only pursuant to orders of the Foreign Intelligence Surveillance Court (FISC) and
is subject to executive, judicial, and Congressional oversight. The DNI emphasized that, under
this program, we do not collect the content of any telephone calls or any information identifying
the callers, nor do we collect cell phone locational information. Rather, the Government obtains
business records created and retained by telecommunication companies for their own internal
purposes, such as billing. The DNI also explained that the Government is authorized to query
the bulk metadata only when there is a reasonable, articulable suspicion, based on specific facts,
that the identifier—e.g., a telephone number—used to query the data is associated with a foreign
terrorist organization previously approved by the FISC. Subsequently, the DNI declassified and
released the FISC's primary order that accompanied the secondary order that had been disclosed in the media, so that the American people could have a more complete picture of the legal parameters under which this activity occurs and the extensive oversight that the FISC requires. The primary order confirms that the Government must adhere to strict limitations on querying, retaining, and disseminating the business records acquired through this program. The Director of NSA also released information concerning the value of the bulk telephony metadata collection program in support of a number of counterterrorism investigations.

In August, the Administration published an extensive white paper to provide more detailed information concerning the section 215 business records program and its legal basis. The white paper explained the process and importance of "contact chaining" under which the NSA may obtain metadata records as many as three "hops" from an identifier associated with a foreign terrorist organization that is used to query the data. It also explained why the telephony metadata collection program meets the "relevance" standard of section 215 and why the program is fully consistent with settled Fourth Amendment law, including the Supreme Court's precedent holding that participants in telephone calls lack a reasonable expectation of privacy in the telephone numbers dialed. Then, in early September the DNI declassified and released more documents concerning the business records program. These documents discuss compliance incidents that were discovered by NSA and DOJ four years ago, reported to the FISC and to the intelligence and judiciary committees, and subsequently resolved. These materials (and others) show that the oversight system worked. The problems were reported to the FISC, the FISC conducted a rigorous review to ensure compliance with its orders and the protection of Americans' privacy, and the Intelligence Community responded effectively.
We have also substantially increased the transparency of the Government’s collection under section 702 of FISA. Even before the recent unauthorized disclosures, the Administration had prepared a public white paper in conjunction with reauthorization of the FISA Amendments Act (FAA) at the end of last year, explaining its intelligence collection activities under the FAA and focusing in particular on collection under section 702. That paper emphasized that section 702 collection targets only non-U.S. persons overseas, and that targeting and minimization procedures and acquisition guidelines are required to ensure that the statutory restrictions are followed and to govern the handling of any U.S. person information that may be incidentally acquired. After the unauthorized disclosures concerning section 702 collection, the DNI refuted much of the inaccurate reporting about the program by releasing a public statement making clear that the Government does not have access to communications carried by U.S. electronic communications service providers without appropriate legal authority. Under section 702 such companies are legally required to provide targeted information to the Government only in response to lawful Government directives, which are issued after the FISC examines and approves certifications required under section 702. The DNI’s statement also explained that the Government cannot collect information under section 702 unless there is an appropriate and documented foreign intelligence purpose, such as preventing terrorism or weapons of mass destruction proliferation.

In August, the DNI declassified and released three opinions from the FISC concerning the section 702 program. As was the case with the section 215 opinions, these opinions concerned a significant compliance incident that caused the Court to criticize the manner in which the section 702 program was being carried out. And, similarly, these opinions provide the
public with considerable insight into the nature and functioning of section 702 collection, while also displaying the detailed and intricate extent of the FISC's review. Indeed, while the FISA statute describes the basic procedures by which the Intelligence Community seeks various authorizations from the FISC, the opinions released reveal fully the thorough, thoughtful, independent review that the FISC provides.

The Administration has taken other steps toward increasing transparency more generally in the context of intelligence collection. For example, the DNI recently introduced a new website called "IC on the Record," which provides ongoing, direct access to information about the foreign intelligence collection activities carried out by the Intelligence Community. Administration officials have also made a number of important public statements relating to the Government's foreign intelligence collection efforts, including a speech by the General Counsel of the Office of the Director of National Intelligence at the Brookings Institution. Moreover, the Government has permitted companies interested in providing greater transparency as to their role in these programs to release certain aggregate statistics about their cooperation with lawful demands from the Government, in a way that will avoid revealing the Government's intelligence collection capabilities with respect to particular providers or platforms. And of course there have been a number of open hearings before committees of the Congress on these issues.

Overall, this is a lot of activity for three months. As we have worked toward greater transparency, we have been mindful of the need to protect intelligence sources and methods. Unfortunately, because of the unauthorized disclosures, a great deal of information that was previously classified about these intelligence programs is now in the public domain. These unauthorized disclosures have already caused significant harm to national security, and
inaccurate or incomplete press coverage of the unauthorized disclosures has also undermined public confidence in our efforts to protect Americans’ privacy. We have to consider these effects as we assess whether additional harm will flow from releasing additional information. There is still substantial information about these activities that can and must remain classified, and we have therefore taken great care to ensure that any documents that are considered for release are carefully reviewed and redacted as appropriate to protect national security. Ultimately, the Government must walk a fine line by disclosing enough information to assure the American public that the Government is acting lawfully but not disclosing so much information that we put the American public in danger.

To complement these transparency efforts, the Administration has taken a series of steps to enhance independent review of U.S. intelligence collection programs. In his August 9 statement, the President noted the importance of the Privacy and Civil Liberties Oversight Board’s (PCLOB’s) review. PCLOB’s statutory mission is “to analyze and review actions the executive branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties.” PCLOB is taking an active role in reviewing the intelligence activities carried out under sections 215 and 702. The Board has received extensive briefings from Administration officials concerning these activities and visited the NSA. In July PCLOB sponsored a public workshop to hear from expert panels and the public.

In his speech in August, President Obama also announced the establishment of a Review Group on Intelligence and Communications Technologies. The Review Group’s task is to advise the President “on how, in light of advancements in technology, the United States can employ its
technical collection capabilities in a way that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure.” The group is charged with conducting an independent review and will report to the President. Group members have received briefings from Administration officials and have met with privacy and civil liberties experts, as well as information technology companies and experts. The group will also be soliciting public comments. The Review Group has been directed to submit an interim report to the President within 60 days and a final report by the end of the year.

Throughout this period, the FISC has continued to exercise its central oversight role with respect to intelligence collection carried out under FISA. In July, ODNI announced that the FISC had renewed its approval for the section 215 program. In connection with that renewal, the FISC has also publicly released an opinion explaining the legal rationale for its decision.

Moreover, as the President discussed in his August 9 statement, the executive branch stands ready to work with Congress to pursue appropriate reforms to section 215, to discuss certain changes to practice before the FISC to ensure that civil liberties concerns have an independent voice in appropriate cases, and to consider efforts at strengthening the transparency of these and other intelligence activities, all in ways consistent with protecting national security. Regarding section 215, we are open to a number of ideas that have been proposed in various quarters to address concerns about the business records program. For example, we would consider statutory restrictions on querying the data that are compatible with operational needs, including perhaps greater limits on contact chaining than what the current FISC orders permit.
We could also consider a different approach to retention periods for the data—consistent with operational needs—and enhanced oversight and transparency measures, such as annual reporting on the number of identifiers used to query the data. To be clear, we believe the manner in which the bulk telephony metadata collection program has been carried out is lawful, and existing oversight mechanisms protect both privacy and security. However, there are some changes that we believe can be made that would enhance privacy and civil liberties as well as public confidence in the program, consistent with our national security needs.

On the issue of FISC reform, we believe that the ex parte nature of proceedings before the FISC is fundamentally sound and has worked well for decades in adjudicating the Government’s applications for authority to conduct electronic surveillance or physical searches in the national security context under FISA. However, we understand the concerns that have been raised about the lack of independent views in certain cases, such as cases involving bulk collection, that affect the privacy and civil liberties interests of the American people as a whole. Therefore, we would be open to discussing legislation authorizing the FISC to appoint an amicus, at its discretion, in appropriate cases, such as those that present novel and significant questions of law and that involve the acquisition and retention of information concerning a substantial number of U.S. persons. Establishing a mechanism whereby the FISC could solicit independent views of an amicus in a subset of cases that raise broader privacy and civil liberties questions, but without compromising classified information, may further assist the Court in making informed and balanced decisions and may also serve to enhance public confidence in the FISC process.
And with regard to enhancing transparency and accountability, the President has directed that the Intelligence Community declassify and make public as much information as possible about certain sensitive intelligence collection programs, including programs undertaken pursuant to sections 215 and 702, while being mindful of the need to protect sensitive classified intelligence and national security. Consistent with that direction, the DNI has directed the Intelligence Community to release publicly, on an annual basis, aggregate information concerning compulsory legal processes under certain national security authorities. We stand ready to discuss whether legislation would be helpful in advancing the President’s objective of ensuring greater transparency for the activities of the Intelligence Community, where consistent with the protection of classified information.

While it is important that we have the aforementioned dialogue about security and civil liberties, we’d also like to take a moment to reiterate some of the comments the President has made about the hard-working men and women of the intelligence community who work every single day to keep us safe because they love this country and believe in its values. These professionals are Americans, too—they come from the same communities, go to the same schools, and care about the same things all Americans do. While the ongoing debate is an important one, and may well result in changes, that dialogue should in no way be perceived as a negative reflection on the dedicated professionals of our Intelligence Community.

We look forward to working with you on these important issues, and we remain grateful for this Committee’s support for these particular intelligence collection programs, which we continue to believe play an important role in our broader foreign intelligence collection efforts. We hope that, with the assistance of this Committee, we can ensure that these programs are on
the strongest possible footing, from the perspective of both national security and privacy, so that they will enjoy broader public and Congressional support in the future. Thank you.
JOINT STATEMENT FOR THE RECORD
OF

JAMES R. CLAPPER
DIRECTOR OF NATIONAL INTELLIGENCE

GENERAL KEITH B. ALEXANDER
DIRECTOR
NATIONAL SECURITY AGENCY
CHIEF
CENTRAL SECURITY AGENCY

JAMES M. COLE
DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
SENATE SELECT COMMITTEE ON INTELLIGENCE

SEPTEMBER 26, 2013
Joint Statement for the Record
of

James R. Clapper
Director of National Intelligence

General Keith B. Alexander
Director, National Security Agency and Chief, Central Security Agency

James M. Cole
Deputy Attorney General
Department of Justice

Before the
Senate Select Committee on Intelligence

September 26, 2013

Thank you for inviting us to discuss the Administration’s efforts to enhance public
confidence in the important intelligence collection programs that have been the subject of
unauthorized disclosures since earlier this year: the collection of bulk telephony metadata under
the business records provision found in section 215 of the USA PATRIOT Act, and the targeting
of non-U.S. persons overseas under section 702 of FISA. We remain committed, as we review
these activities, both to ensuring that we have the authorities we need to collect important foreign
intelligence to protect the country from terrorism and other threats to national security, and to
protecting privacy and civil liberties in a manner consistent with our values. We also remain
committed to working closely with this Committee as any modifications to these activities are considered. We understand that some of the initiatives announced by the President in his statement on August 9 are of interest to the Committee, and we welcome the opportunity to discuss them with you and to work together in moving forward.

The first step in promoting greater public confidence in these intelligence activities is to provide greater transparency so that the American people understand what the activities are, how they function, and how they are overseen. As you know, many of the reports appearing in the media concerning the scope of the Government's intelligence collection efforts have been inaccurate, including with respect to the collection carried out under sections 215 and 702. In response, the Administration has released substantial information since June to increase transparency and public understanding, while also working to ensure that these releases are consistent with national security.

We have worked to provide the public greater insight into the operation of the bulk telephony metadata business records collection program under section 215. In early June, the Director of National Intelligence (DNI) released a public statement explaining that the program is carried out only pursuant to orders of the Foreign Intelligence Surveillance Court (FISC) and is subject to executive, judicial, and Congressional oversight. The DNI emphasized that, under this program, we do not collect the content of any telephone calls or any information identifying the callers, nor do we collect cell phone locational information. Rather, the Government obtains business records created and retained by telecommunication companies for their own internal purposes, such as billing. The DNI also explained that the Government is authorized to query the bulk metadata only when there is a reasonable, articulable suspicion, based on specific facts,
that the identifier—e.g., a telephone number—used to query the data is associated with a foreign terrorist organization previously approved by the FISC. Subsequently, the DNI declassified and released the FISC’s primary order that accompanied the secondary order that had been disclosed in the media, so that the American people could have a more complete picture of the legal parameters under which this activity occurs and the extensive oversight that the FISC requires. The primary order confirms that the Government must adhere to strict limitations on querying, retaining, and disseminating the business records acquired through this program. The Director of NSA also released information concerning the value of the bulk telephony metadata collection program in support of a number of counterterrorism investigations.

In August, the Administration published an extensive white paper to provide more detailed information concerning the section 215 business records program and its legal basis. The white paper explained the process and importance of “contact chaining” under which the NSA may obtain metadata records as many as three “hops” from an identifier associated with a foreign terrorist organization that is used to query the data. It also explained why the telephony metadata collection program meets the “relevance” standard of section 215 and why the program is fully consistent with settled Fourth Amendment law, including the Supreme Court’s precedent holding that participants in telephone calls lack a reasonable expectation of privacy in the telephone numbers dialed. Then, in early September the DNI declassified and released more documents concerning the business records program. These documents discuss compliance incidents that were discovered by NSA and DOJ four years ago, reported to the FISC and to the intelligence and judiciary committees, and subsequently resolved. These materials (and others) show that the oversight system worked. The problems were reported to the FISC, the FISC
conducted a rigorous review to ensure compliance with its orders and the protection of Americans' privacy, and the Intelligence Community responded effectively.

We have also substantially increased the transparency of the Government’s collection under section 702 of FISA. Even before the recent unauthorized disclosures, the Administration had prepared a public white paper in conjunction with reauthorization of the FISA Amendments Act (FAA) at the end of last year, explaining its intelligence collection activities under the FAA and focusing in particular on collection under section 702. That paper emphasized that section 702 collection targets only non-U.S. persons overseas, and that targeting and minimization procedures and acquisition guidelines are required to ensure that the statutory restrictions are followed and to govern the handling of any U.S. person information that may be incidentally acquired. After the unauthorized disclosures concerning section 702 collection, the DNI refuted much of the inaccurate reporting about the program by releasing a public statement making clear that the Government does not have access to communications carried by U.S. electronic communications service providers without appropriate legal authority. Under section 702 such companies are legally required to provide targeted information to the Government only in response to lawful Government directives, which are issued after the FISC examines and approves certifications required under section 702. The DNI's statement also explained that the Government cannot collect information under section 702 unless there is an appropriate and documented foreign intelligence purpose, such as preventing terrorism or weapons of mass destruction proliferation.

In August, the DNI declassified and released three opinions from the FISC concerning the section 702 program. As was the case with the section 215 opinions, these opinions
concerned a significant compliance incident that caused the Court to criticize the manner in which the section 702 program was being carried out. And, similarly, these opinions provide the public with considerable insight into the nature and functioning of section 702 collection, while also displaying the detailed and intricate extent of the FISC’s review. Indeed, while the FISA statute describes the basic procedures by which the Intelligence Community seeks various authorizations from the FISC, the opinions released reveal fully the thorough, thoughtful, independent review that the FISC provides.

The Administration has taken other steps toward increasing transparency more generally in the context of intelligence collection. For example, the DNI recently introduced a new website called “IC on the Record,” which provides ongoing, direct access to information about the foreign intelligence collection activities carried out by the Intelligence Community. Administration officials have also made a number of important public statements relating to the Government’s foreign intelligence collection efforts, including a speech by the General Counsel of the Office of the Director of National Intelligence at the Brookings Institution. Moreover, the Government has permitted companies interested in providing greater transparency as to their role in these programs to release certain aggregate statistics about their cooperation with lawful demands from the Government, in a way that will avoid revealing the Government’s intelligence collection capabilities with respect to particular providers or platforms. And of course there have been a number of open hearings before committees of the Congress on these issues.

Overall, this is a lot of activity for three months. As we have worked toward greater transparency, we have been mindful of the need to protect intelligence sources and methods. Unfortunately, because of the unauthorized disclosures, a great deal of information that was
previously classified about these intelligence programs is now in the public domain. These unauthorized disclosures have already caused significant harm to national security, and inaccurate or incomplete press coverage of the unauthorized disclosures has also undermined public confidence in our efforts to protect Americans' privacy. We have to consider these effects as we assess whether additional harm will flow from releasing additional information. There is still substantial information about these activities that can and must remain classified, and we have therefore taken great care to ensure that any documents that are considered for release are carefully reviewed and redacted as appropriate to protect national security. Ultimately, the Government must walk a fine line by disclosing enough information to assure the American public that the Government is acting lawfully but not disclosing so much information that we put the American public in danger.

To complement these transparency efforts, the Administration has taken a series of steps to enhance independent review of U.S. intelligence collection programs. In his August 9 statement, the President noted the importance of the Privacy and Civil Liberties Oversight Board's (PCLOB's) review. PCLOB's statutory mission is "to analyze and review actions the executive branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties." PCLOB is taking an active role in reviewing the intelligence activities carried out under sections 215 and 702. The Board has received extensive briefings from Administration officials concerning these activities and visited the NSA. In July PCLOB sponsored a public workshop to hear from expert panels and the public.
In his speech in August, President Obama also announced the establishment of a Review Group on Intelligence and Communications Technologies. The Review Group’s task is to advise the President “on how, in light of advancements in technology, the United States can employ its technical collection capabilities in a way that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure.” The group is charged with conducting an independent review and will report to the President. Group members have received briefings from Administration officials and have met with privacy and civil liberties experts, as well as information technology companies and experts. The group will also be soliciting public comments. The Review Group has been directed to submit an interim report to the President within 60 days and a final report by the end of the year.

Throughout this period, the FISC has continued to exercise its central oversight role with respect to intelligence collection carried out under FISA. In July, ODNI announced that the FISC had renewed its approval for the section 215 program. In connection with that renewal, the FISC has also publicly released an opinion explaining the legal rationale for its decision.

Moreover, as the President discussed in his August 9 statement, the executive branch stands ready to work with Congress to pursue appropriate reforms to section 215, to discuss certain changes to practice before the FISC to ensure that civil liberties concerns have an independent voice in appropriate cases, and to consider efforts at strengthening the transparency of these and other intelligence activities, all in ways consistent with protecting national security. Regarding section 215, we are open to a number of ideas that have been proposed in various
quarters to address concerns about the business records program. For example, we would consider statutory restrictions on querying the data that are compatible with operational needs, including perhaps greater limits on contact chaining than what the current FISC orders permit. We could also consider a different approach to retention periods for the data—consistent with operational needs—and enhanced oversight and transparency measures, such as annual reporting on the number of identifiers used to query the data. To be clear, we believe the manner in which the bulk telephony metadata collection program has been carried out is lawful, and existing oversight mechanisms protect both privacy and security. However, there are some changes that we believe can be made that would enhance privacy and civil liberties as well as public confidence in the program, consistent with our national security needs.

On the issue of FISC reform, we believe that the ex parte nature of proceedings before the FISC is fundamentally sound and has worked well for decades in adjudicating the Government's applications for authority to conduct electronic surveillance or physical searches in the national security context under FISA. However, we understand the concerns that have been raised about the lack of independent views in certain cases, such as cases involving bulk collection, that affect the privacy and civil liberties interests of the American people as a whole. Therefore, we would be open to discussing legislation authorizing the FISC to appoint an amicus, at its discretion, in appropriate cases, such as those that present novel and significant questions of law and that involve the acquisition and retention of information concerning a substantial number of U.S. persons. Establishing a mechanism whereby the FISC could solicit independent views of an amicus in a subset of cases that raise broader privacy and civil liberties questions, but without compromising classified information, may further assist the Court in
making informed and balanced decisions and may also serve to enhance public confidence in the FISC process.

And with regard to enhancing transparency and accountability, the President has directed that the Intelligence Community declassify and make public as much information as possible about certain sensitive intelligence collection programs, including programs undertaken pursuant to sections 215 and 702, while being mindful of the need to protect sensitive classified intelligence and national security. Consistent with that direction, the DNI has directed the Intelligence Community to release publicly, on an annual basis, aggregate information concerning compulsory legal processes under certain national security authorities. We stand ready to discuss whether legislation would be helpful in advancing the President’s objective of ensuring greater transparency for the activities of the Intelligence Community, where consistent with the protection of classified information.

While it is important that we have the aforementioned dialogue about security and civil liberties, we’d also like to take a moment to reiterate some of the comments the President has made about the hard-working men and women of the intelligence community who work every single day to keep us safe because they love this country and believe in its values. These professionals are Americans, too—they come from the same communities, go to the same schools, and care about the same things all Americans do. While the ongoing debate is an important one, and may well result in changes, that dialogue should in no way be perceived as a negative reflection on the dedicated professionals of our Intelligence Community.

We look forward to working with you on these important issues, and we remain grateful for this Committee’s support for these particular intelligence collection programs, which we
continue to believe play an important role in our broader foreign intelligence collection efforts. We hope that, with the assistance of this Committee, we can ensure that these programs are on the strongest possible footing, from the perspective of both national security and privacy, so that they will enjoy broader public and Congressional support in the future. Thank you.
PROJECTING FORCE IN THE 21ST CENTURY - LEGITIMACY AND THE RULE OF LAW

TITLE 50, TITLE 10, TITLE 18, AND ART. 75

Jeff Mustin* & Harvey Rishikof**

I. PROLOGUE: THE MODERN BATTLEFIELD ........................................ 1235
II. EXPERTS ON THE ISSUES .............................................................. 1236
III. LEGAL AUTHORITY FOR COVERT ACTION ............................... 1240
IV. WHO MAY CONDUCT A COVERT ACTION? ................................. 1242
IV. ADDITION BY SUBTRACTION: WHAT IS A TRADITIONAL
MILITARY ACTIVITY?................................................................. 1243
V. POLICY IMPLICATIONS .................................................................. 1245
VII. PROSECUTION V. LETHALITY - TITLE 18, ART. 75 AND RULE OF
LAW ................................................................................................... 1247
VIII. CONCLUSION ............................................................................... 1251

I. PROLOGUE: THE MODERN BATTLEFIELD

The Prussian strategist Carl von Clausewitz wrote that the first duty of the general and statesman is to understand the nature of the war upon which they are embarking.1 The modern battlefield has complicated this task. The United States military is currently conducting simultaneous counterinsurgency and counterterrorism operations in Afghanistan and Pakistan (“AF/PAK”),2 while the


**  B.A., McGill University (1975); M.A. Brandeis University (1978); J.D., New York University (1996). Chair of the ABA Standing Committee on Law and National Security. Former professor of law and chair, Department of National Security Strategy, National War College. The views expressed in this Article are those of the author and do not reflect the official policy or position of the National Defense University, the National War College, the Department of Defense, the Director of National Intelligence, or the U.S. government.


Central Intelligence Agency ("CIA"), traditionally more concerned with espionage than air warfare, has been conducting a robust aerial attack campaign in Pakistan’s Northwest Frontier Province.\(^3\) Conventional military forces, special operations forces, and intelligence professionals are all operating in the same area of operations, trying to enact the same strategies to meet the same policy goals but using contradictory legal authorities to do so.\(^4\)

The modern battlefield, defined in this Article as military operations since 2001, has contributed to the operational synthesis of intelligence and military organizations. The recent news that America’s most visible general officer, David Petraeus, will head the CIA and the former Director of the CIA, Leon Panetta, will take charge of the Department of Defense ("DoD"), illustrates a growing synergy between the nation’s primary spy agency and the military.\(^5\)

The melding of executive agency roles and missions recently prompted national security writer and senior fellow at the Council on Foreign Relations, Max Boot, to opine that, "[w]e’re in an era of ‘covert action.’"\(^6\) But what exactly is covert action?

Perhaps Clausewitz’s guidance to understanding the nature of the counterinsurgency or counterterrorism fight is a difficult but achievable goal; understanding which forces to apply to which fight and what legal authorities authorize such action seems almost impossible. This Article seeks to clarify which forces are legally appropriate for which missions by defining and analyzing the differences between traditional military activities ("TMAs") and covert actions, and the consequences for prosecution. The first step to achieve this goal is to hear what the experts themselves say.

II. EXPERTS ON THE ISSUES

Experts in TMA and covert action convened in May to discuss legal authorities. The event, entitled "The bin Laden Operation – The Legal Framework" and sponsored by the American Bar Association’s Standing Committee on Law and National Security, provided a forum to dissect when operations fall under Title 10 versus Title 50 authorities. The event summary is instructive for this Article:

[T]he panelists addressed whether the bin Laden operation


\(^6\) Max Boot, *Covert Action Makes a Comeback*, WALL ST. J., Jan. 5, 2011, at A15 (stating that "covert action can be a valuable part of the policy maker’s tool kit, provided that it is integrated into a larger plan").
had been properly designated a Title 50 operation rather than one under Title 10 authority. The panel included Syracuse Law professor William C. Banks; Senior Advisor to the Director of Operations for U.S. Cyber Command, Eric Greenwald; former Acting CIA General Counsel, John Rizzo; and, Deputy Legal Counsel, Office of the Chairman of the Joint Chiefs of Staff, Captain Stephanie Smart. Moderating the discussion was Special Advisor to the Committee, and Principal at Bingham Consulting Group, Suzanne Spaulding.

... [Professor Banks] began by noting that soon after the bin Laden operation was conducted, CIA Director Leon Panetta explained that it was a Title 50 operation and not Title 10. Professor Banks then defined “covert action” as an activity carried out by the United States government that is meant to influence political, economic, or military conditions abroad and where the role of the U.S. government will not be apparent or publicly acknowledged. He went on to highlight the major exceptions to 413b’s requirements which are traditional counter-intelligence or police activities and traditional military activities. U.S. government entities carrying out these types of activities are not bound by 413b’s requirements.

The traditional military activities exception (TMA) became a central issue of discussion for the panel as it was directly related to the bin Laden operation and has long been an area of confusion and concern vis-à-vis the oversight of covert activity. Professor Banks expressed skepticism as to how the bin Laden operation could be considered a Title 50 operation when the force that executed the mission was primarily military personnel from SEAL Team Six (or DEVGRU, as it is now known), and was commanded by Vice Admiral William McRaven, commander of the U.S. Joint Special Operations Command. He pointed out that a specific element of a TMA is that it be under the direction and control of a military commander which this operation was, thus making the bin Laden raid a TMA under Title 10 and not a covert action under Title 50.

The next panelist to speak was former Acting CIA General Counsel, John Rizzo. He emphasized that covert operations are not solely the purview of the CIA, and that any U.S. government agency is technically authorized to carry out a covert operation provided that they comply with 413b, but Mr. Rizzo could not recall a single instance in his many years of dealing with this issue in which an agency other than the CIA sought and received the required written finding to conduct a covert action – even the U.S. military. (Later, during the Q & A session, Rizzo and Eric Greenwald further explained that this is partly because the CIA is the only

agency equipped with the internal legal mechanisms to easily comply with the oversight requirements of 413b.)

Rizzo also discussed the period during which Congress attempted to codify a statutory framework for covert actions (1990-91) and noted that creating a formal definition for “traditional military activity” had been exceedingly difficult. The definition of a TMA is not explicit in 413b, but legislative history lays out the elements as an activity being a TMA if it is: 1) conducted by military personnel; 2) under the direction and control of a U.S. military commander; 3) preceding or related to hostilities which are either anticipated to involve U.S. military forces, or where such hostilities are ongoing; and, 4) where the U.S. role in the overall operation is apparent or acknowledged publicly.  

Next to speak was Captain Stephanie Smart . . . . She noted that military and CIA operations are equally subject to Congressional oversight, but that the TMA exception allows for a wide range of military operations not subject to 413b. She questioned Professor Banks’ assertion that the bin Laden raid had been exclusively a Title 10 action because it was conducted under the direction and control of a military commander; Capt. Smart countered by pointing out multiple elements that can define a TMA, not just military “command and control.” She further opined that the bin Laden operation could have been carried out under Title 10 or Title 50, and that the mere involvement of the military does not exclude it from the realm of Title 50 . . . .

The last panelist to speak was Eric Greenwald, whose current job is as a senior advisor to the military’s new Cyber Command . . . . Mr. Greenwald stated that during his time on the Hill, he encountered the blurry distinction between Title 10 and Title 50 authorities with regard to military operations termed “operational preparation of the environment” and intelligence activities under Title 50. While Title 50 intelligence activities are different than covert actions, this gave Mr. Greenwald experience with the often confusing interplay between Title 10 and Title 50; however, he stated that his current work with DoD has shown him how much care the military takes in ensuring that all operations are scrutinized to determine whether they properly fall under Title 10 or Title 50.

. . . . The discussion and audience questions that followed the panelists’ opening remarks continued to swirl around the TMA exception to 413b . . . . Professor Banks and Mr. Greenwald both agreed that the definition of a TMA is a moving target.

---

and that Congress may have intentionally meant the definition to be vague so as to allow flexibility in this area . . . . However, Mr. Greenwald pointed out that an action is not a TMA just because it is carried out by the military and that any such blanket characterization could likely thwart the congressional intent behind 413b of providing additional oversight to the type of paramilitary operations that had been carried out by CIA in the decades preceding the creation of these provisions in 1991.

One of Capt. Smart’s final points highlighted the DoD’s institutional process when it comes to the Title 10 versus Title 50 determination. Earlier in the discussion she pointed out that the department has a number of deconfliction mechanisms to vet operations to make sure that they are conducted under the appropriate legal authority. Later she stated that to her knowledge DoD has never sought a presidential finding for covert action under 413b. If DoD decides that an operation may more properly fall under Title 50, it does not conduct the operation or approaches the CIA and offers to turn the operation over. If the CIA accepts the operation then it will put together the required written finding and it will be conducted as a CIA operation with the military providing support on some level.

The last short issue discussed was the possibility of a “Title 60” that would basically consolidate Title 10 and Title 50 in an attempt to clarify legal boundaries in the area of covert action. The major proponent of this plan was former Director of National Intelligence, Dennis Blair, who suggested this both during his confirmation hearing and during testimony at a recent congressional hearing. The idea of Title 60 would be to provide a more clear legal framework for joint covert activities such as the bin Laden operation.9

Not discussed by the panel was what would have happened if Osama bin Laden had been arrested, returned to the United States, and prosecuted under criminal law, Title 18.10 Another option would have been to use the military commissions structure.11 From a legal perspective, it is important to note there was an outstanding arrest warrant for bin Laden in the Southern District of New York for his involvement in 9/11, and during the last ten years, he remained on

the Federal Bureau of Intelligence ("FBI") Top Ten list. Since 9/11, there has been a robust debate among the three branches of our government as to the proper way to detain and prosecute detainees from the war on terrorism. At the time of this Article, the constitutionality of military commissions or the need for a special national security court still remain unclear. Under international law, there are due process regimes for prosecution that have been recognized as legitimate forums for adjudication in complex hostile situations, such as Article 75 under Additional Protocol I.¹²

As the panel discussion reflects, there is much confusion and debate on how to conceptualize the projection of force in the twenty-first century where traditional military activities and covert operations are merging. Moreover, how prosecution and detention fit our strategic approach to combat extremism has not yet been integrated into a holistic plan. Should these legitimate targets, if detained, be treated as traditional criminals, war criminals, or held as prisoners of war? Moreover, what is the best forum for trial: civil courts, military commissions, a special national security court, a foreign court, or an international court? Much of this confusion flows from the confusion of defining the modern battlefield.

III. LEGAL AUTHORITY FOR COVERT ACTION

The word "covert" carries important connotations. The term, in its colloquial usage, is frequently used to describe any activity the government wants concealed from the public eye, a usage that carries with it implications of illicit activity. However, legal usage of the word "covert" rarely evokes illicit connotations; in fact, the lawfulness of covert action is rarely debated at all. According to one treatise on covert action, "there has been a remarkably consistent national policy in favor of maintaining a competence to conduct a wide range of covert operations . . . . The national debate has, thus, focused not on the lawfulness of covert action but on the constitutional allocation of competence to control it."¹³ The real issue is over accountability and the role of the covert action from a policy perspective.

The ability to control covert action begins with its legal definition. The term "covert action" is statutorily defined as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be

---


apparent or acknowledged publicly . . .”14 The DoD defines covert action similarly, stating that a covert action is “[a]n operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor.”15 Both definitions focus on concealing the identity of the activity’s sponsor.

As important as it is to define what covert action is, it is equally important to define what covert action is not. Statutorily, covert action does not include:

1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
2) traditional diplomatic or military activities or routine support to such activities;
3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.16

Additionally, covert action is prohibited if it is “intended to influence United States political processes, public opinion, policies, or media.”17

Thus, because of 50 U.S.C. § 413b(e)(1), intelligence activities are not generally considered covert activities. Instead, intelligence collection is generally considered clandestine in nature.18 The DoD defines clandestine activities as “[a]n operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment.”19 Simply put, covert action

15. Joint Chiefs of Staff, Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms 132 (2001) (“A covert operation differs from a clandestine operation in that emphasis is placed on concealment of the identity of the sponsor rather than on concealment of the operation.”).
17. 50 U.S.C. § 413b(f).
18. See 50 U.S.C. §§ 403-04a(f) (“Under the direction of the Director of National Intelligence and in a manner consistent with section 3927 of Title 22, the Director of the Central Intelligence Agency shall coordinate the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.”).
19. Joint Chiefs of Staff, Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms 89 (2001) (“In special operations, an activity may be both covert and clandestine and may focus equally on operational
conceals the identity of the country involved in an operation; clandestine activity hides the very existence of the operation.

IV. WHO MAY CONDUCT A COVERT ACTION?

Ultimately, the ability to conduct covert action lies with the CIA, with some notable exceptions. The initial power to conduct covert action is granted to the Executive through 50 U.S.C. §§ 403-4a(d), which provides the CIA with the authority to collect, correlate, evaluate, and coordinate intelligence collection. Additionally, in pertinent part, the CIA is authorized to “perform such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct.” This is the so-called “Fifth Function,” or implicit authorization for the CIA to conduct covert action.

This power is defined more explicitly within Executive Order 12,333, which states:

[The CIA shall . . . . conduct [covert action] activities approved by the President. No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution (87 Stat. 855)) may conduct any [covert action] activity unless the President determines that another agency is more likely to achieve a particular objective . . . .]

This provides the CIA with clear executive authority to conduct covert action pursuant to a presidential finding. Interestingly, however, there are two major caveats. The first caveat provides for U.S. Armed Forces covert action pursuant to a declaration of war by Congress, or “during any period covered by a report from the President to the Congress under the War Powers Resolution.” The second caveat provides that another agency—any other agency—may conduct a covert action if that other agency would be “more likely to

considerations and intelligence-related activities.”).

20. 50 U.S.C. §§ 403-04a(1)-(4).
21. Id. §§ 403-04a(d)(4).
24. Id. at 5546. No president has ever acknowledged being bound by the War Powers Resolution, but this executive order makes it clear that any military action “consistent with” but not binding the Executive, will suffice. See also Berney Dycus et al., NATIONAL SECURITY LAW 250-51 (4th ed. 2007) (stating that President Ford reported to Congress “taking note of the provision of Section 4(a)(2) of the War Powers Resolution;” President Carter reported “consistent with the reporting provisions of the War Powers Resolution.”) (internal citations omitted).
achieve [the] particular objective.”\textsuperscript{25} For example, if the Department of Energy had particular expertise in detecting nuclear radiation, it might be authorized, via presidential finding, to conduct a covert action relating to detecting nuclear radiation.

This second caveat opens the door for any agency, including Special Operations Forces (“SOF”), to conduct covert action. The DoD agrees. Joint Publication 3-05.2 defines yet another type of mission that leaves the door open for alternative uses for SOF: collateral missions.\textsuperscript{26} Collateral missions are “mission[s] other than those for which a force is primarily organized, trained, and equipped, that the force can accomplish by virtue of the inherent capabilities of that force.”\textsuperscript{27} The executive summary to Joint Publication 3-05.2 explains, “SOF conduct specific principal missions and can conduct collateral activities using the inherent capabilities resident in the primary missions.”\textsuperscript{28} Thus, depending on the type of missions, SOF might be the primary choice for covert action if they have inherent capabilities superior to those of the CIA for a particular mission.

In summary, a covert action may be conducted by any agency the President deems appropriate. While the CIA clearly would be the primary agency to perform the Fifth Function, any agency may be authorized by presidential finding to conduct covert action exclusive of the limitations in 50 U.S.C. § 413b(e)(1)-(4). In short, the statute affords the President multiple potential choices, but the issue of accountability remains.

IV. ADDITION BY SUBTRACTION: WHAT IS A TRADITIONAL MILITARY ACTIVITY?

As previously discussed, defining covert action requires an understanding of what covert action is and is not. Referring back to 50 U.S.C. §§ 413b(e)(1)-(4), covert action is statutorily segregated from traditional intelligence and counterintelligence activities, traditional military activities, traditional law enforcement activities, and “activities to provide routine support to the overt activities.”\textsuperscript{29}

Implicitly, this list of “traditional” activities would seem to indicate that covert action was never meant to be traditional. Instead, it was meant to provide policy makers with an option on the “continuum between diplomacy and war.”\textsuperscript{30} Covert action has not

\textsuperscript{26} Joint Chiefs of Staff, Joint Publication 3-05.2, Joint Tactics, Techniques and Procedures for Special Operations Targeting and Mission Planning GL-6 (2003).
\textsuperscript{27} Id.
\textsuperscript{28} Id. at xi.
\textsuperscript{29} 50 U.S.C. § 413b(e)(1)-(4).
always been a prominent policy tool; “covert action was not an integral policy tool until the Cold War.”

Applying this to the modern battlefield, if covert action is not a traditional military activity, then what is a traditional military activity? There is no legal definition. If one sought to define traditional military activities through historical practice, he or she might look to doctrinal or customary missions. A hypothetical list of such activities might include maneuver warfare, aerial attack, artillery barrages, or amphibious landings. However, this list is problematic because the tactics, techniques, and procedures involved with warfare are constantly changing. Prior to 2001, few would have listed counterinsurgency as a primary mission set of the conventional United States Army. Similarly, a decade ago, few security experts would have listed cyberwarfare among traditional military activities. Consequently, the term “traditional” makes merging historical military practice and modern combat realities difficult in an adaptive environment like war. To compound matters, it is extremely difficult to predict the nature of the next war or even the next evolution of the current war. The adaptive nature of war may or may not drive activities that lie within “traditional” military missions. As a result, looking to doctrinal or customary missions does not help one looking for a legal definition of a traditional military action.

Instead, in absence of positive guidance about what constitutes a traditional military activity, the most precise language can be devised by analyzing what is the absence of covert action. Defining a traditional military activity this way would consist of two elements: 1) those activities on the battlefield that are not covert action and are not authorized by presidential finding but, 2) that are authorized under traditional jus ad bellum sources. Stated another way, traditional military activities would be overt actions (or covert actions not requiring a presidential finding such as preparations for war) authorized under jus ad bellum.

31. Id. at 148 (“Such ‘covert’ mechanisms allowed proxies to engage in hot war, while the great power conflict remained ‘cold.’”).
33. Such jus ad bellum sources might include United Nations Charter Article 42 or 51 actions, or congressional declarations of war. See U.N. Charter arts. 42, 51.
V. POLICY IMPLICATIONS

If these definitions are accepted as true, the result is that it has become legally easier for the executive branch to order covert action than to order conventional armed conflict. To commit military troops for a traditional military action, the President must have a *casus belli* and subsequently seek *jus ad bellum* justification and (typically) international support. This would usually involve the political and diplomatic gyrations involved in garnering both domestic legal support from Congress and international legal support from the United Nations Security Council.

Alternatively, to authorize a covert action, the President may forgo these diplomatic and political gyrations and merely issue a classified finding to conduct a covert action. While the President must report this action to Congress, the President may restrict disclosure to the “Gang of Eight” when “it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States . . . .”

Thus, while covert action is not without legal accountability, it is a much more direct way for the President to commit forces. Additionally, forces conducting covert action operate by stealth. By their nature, they will have much lower visibility in the public eye. This provides the Executive a lawful option to commit force while theoretically lessening the media accountability for those actions. As a result, covert action also vests an immense amount of authority in the Executive and the “Gang of Eight” to conduct operations without the accountability to their constituents typically found in a democratic society.

Covert action also enables unilateral action. The stealthy nature

34. See 50 U.S.C. § 413b(b) (“To the extent consistent with due regard for the protection from unauthorized disclosure of classified information . . . the Director of National Intelligence . . . (1) shall keep the congressional intelligence committees fully and currently informed of all covert actions . . . ; and (2) shall furnish to the congressional intelligence committees any information or material concerning covert actions . . . which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.”).

35. 50 U.S.C. § 413b(c)(2). The “Gang of Eight” consists of “the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, [] the majority and minority leaders of the Senate . . . . [and] other . . . members of the congressional leadership . . . may be included by the President.” Id.

36. See New York Times Co. v. United States, 403 U.S. 713, 719 (1971) (Black, J., concurring). “Secrecy in government is fundamentally anti-democratic, perpetuating bureaucratic errors. Open debate and discussion of public issues are vital to our national health.” Id. at 724. “[T]he only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in . . . informed and critical public opinion which alone can here protect the values of democratic government.” Id. at 728 (Stewart, J., concurring).
of covert action means that the Executive would be discouraged from seeking international cooperation. Any international support would likely be limited to notifying host nations of the presence of troops, and those notifications, as a tactical matter, would likely be last minute and very directive in nature.\footnote{Notification of covert infiltration, as a practical matter, renders the covert nature of the action null. See Reisman & Baker, supra note 13, at 14.} This type of unilateral action contrasts the cooperative intent for international law,\footnote{See U. N. Charter art. 2, para. 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").} and, in the words of one legal scholar, "[u]nilateral action- covert or overt - generates particularly high emotions, because many view it as a litmus test for one’s commitment to international law."\footnote{Reisman & Baker, supra note 13, at 3.} Excessive use of covert action might be deemed by some nations as a rebuke of international law or evidence of a hubristic foreign policy. The continued and constant use of this instrument when lethality is the goal raises issues of international legitimacy.

Despite these reservations, covert action can be a useful policy tool. It is much more flexible and rapid than a traditional military activity, meaning it is much more suited to countering an adaptive enemy.\footnote{See generally Stanley A. McChrystal, It Takes a Network, FOREIGN POLICY, Mar.-Apr. 2011.} Covert operations are generally more acute in their scope and objectives, which provides policymakers a scalpel to apply instead of the massive hammer of the U.S. military. Also, there are times when foreign policy maneuvers require stealth. One might imagine the need to retrieve unsecured nuclear material as a mission requiring immediacy and discreetness inappropriate for a large military unit.

A textbook case of covert action as a useful policy tool was the May 2011 raid on the compound of Osama bin Laden. The direct action strike was a Title 50 action conducted by DoD special operations assets.\footnote{Kimberly Dosier & Robert Burns, Raid Raises Question: Who’s Soldier, Who’s Spy?, FOX NEWS (May 5, 2011), http://www.foxnews.com/us/2011/05/05/raid-raises-question-whos-soldier-whos-spy/.} The likely legal scenario for this operation was that President Obama issued his finding, which authorized the CIA to “own” the operation and, under subsequent Title 50 authorities, allowed Joint Special Operations Command to conduct the raid because the President determined “that another agency is more likely to achieve a particular objective . . . .”\footnote{See Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,945-46 (Dec. 4, 1981); see also Sean D. Naylor, Bin Laden raid a triumph for Spec Ops, ARMY TIMES, May 9, 2011 (describing some of the unique capabilities that might cause special operations
even from the host nation, was obvious, and the covert action provided the acute desired result.

While the bin Laden raid demonstrates a positive result and the operation shows a clear need to maintain an ability to conduct covert action, it is important to emphasize that covert action is not without policy hazards. The danger in blurring the line between covert action and traditional military activities is that policymakers will choose to authorize what might normally be characterized as a traditional military activity under the guise of a covert action in order to circumvent the need for accountability or international support. Applying traditional military force without transparency is not the \textit{raison d’être} for a covert capability.

For a case study, one need not look further than our current military conflict in AF/PAK. Is the precision bombing campaign being conducted truly a traditional military activity or a covert action? While arguments can be made for both sides, the mission of precision bombing, especially over an extended duration, has traditionally fallen to the United States Air Force or United States Navy. The action, despite its legal authorization, is certainly overt; newspapers chronicle the airstrikes daily. One must wonder, then, how the concept of “covert” is being understood on the modern battlefield.

VII. Prosecution v. Lethality - Title 18, Art. 75 and Rule of Law

The use of lethality versus capture and prosecution in the covert action context raises the difficult questions of grand strategy and the final goals of the decision to project force. Unless the state has created a legitimate prosecutorial due process regime that is recognized both domestically and internationally, the missions of lethality raise the question of international sovereignty and compliance with host nation laws. These missions are potentially taking place in territories that are not per se war zones or not clearly recognized battlefields in the traditional sense. Lethality against either citizens of the host nation or noncitizens there illegally or legally, raises fundamental questions about the rule of law. Why is capture for prosecution not the first option? In international law, there is much discussion of “international armed conflicts” versus “non-international armed conflicts.” The categorization of these

\footnotesize{forces to be chosen over CIA assets).

conflicts flows from Additional Protocol I and Additional Protocol II, 44 two conventions the United States has declined to ratify at this time. In a non-international armed conflict under Additional Protocol I, the host state may have to accord Geneva Convention rights to the "rebels" as perceived by the host state. 45 Whether the "rebel" is a legitimate target turns on a number of facts, including whether the individual is a "direct participant in hostilities," a designation that is hotly debated in international circles. 46 In situations of some ambiguity, without capture as an option and some due process, how is the shooter sure the target is the legitimate target? Moreover, two of the principles of the law of armed conflict are the principle of distinction between combatants and civilians and the requirement of proportionality to minimize noncombatant causalities.

If capture becomes an option for strategic reasons, then a choice of using criminal courts, military commissions, special national security courts, host courts, or an international tribunal are then raised. Regardless of the court employed, the issue of appropriate due process is the central question. What is critical is that the process has legitimacy and comports with rule of law. To this end, Additional Protocol I Article 75 establishes the basic due process for individuals captured in conflict situations and deserves to be quoted in full so that the basic rights it entails are understood. It reads as follows:

Article 75—Fundamental guarantees

1. In so far as they are affected by a situation referred to in Article 1 of this Protocol, persons who are in the power of a Party to the conflict and who do not benefit from more favourable treatment under the Conventions or under this Protocol shall be treated humanely in all circumstances and shall enjoy, as a minimum, the protection provided by this Article without any adverse distinction based upon race, colour, sex, language, religion or belief, political or other opinion, national or social origin, wealth, birth or other status, or on any other similar criteria. Each Party shall respect the person, honour, convictions and religious practices of all such persons.

2. The following acts are and shall remain prohibited at any time and in any place whatsoever, whether committed by civilian or by military agents:

(a) Violence to the life, health, or physical or mental well-being

46. See Protocol II, supra note 44, art. 13.
of persons, in particular:

(i) Murder;
(ii) Torture of all kinds, whether physical or mental;
(iii) Corporal punishment; and
(iv) Mutilation;
(b) Outrages upon personal dignity, in particular humiliating and degrading treatment, enforced prostitution and any form of indecent assault;
(c) The taking of hostages;
(d) Collective punishments; and
(e) Threats to commit any of the foregoing acts.

3. Any person arrested, detained or interned for actions related to the armed conflict shall be informed promptly, in a language he understands, of the reasons why these measures have been taken. Except in cases of arrest or detention for penal offences, such persons shall be released with the minimum delay possible and in any event as soon as the circumstances justifying the arrest, detention or internment have ceased to exist.

4. No sentence may be passed and no penalty may be executed on a person found guilty of a penal offence related to the armed conflict except pursuant to a conviction pronounced by an impartial and regularly constituted court respecting the generally recognized principles of regular judicial procedure, which include the following:

(a) The procedure shall provide for an accused to be informed without delay of the particulars of the offence alleged against him and shall afford the accused before and during his trial all necessary rights and means of defence;
(b) No one shall be convicted of an offence except on the basis of individual penal responsibility;
(c) No one shall be accused or convicted of a criminal offence on account of any act or omission which did not constitute a criminal offence under the national or international law to which he was subject at the time when it was committed; nor shall a heavier penalty be imposed than that which was applicable at the time when the criminal offence was committed; if, after the commission of the offence, provision is made by law for the imposition of a lighter penalty, the offender shall benefit thereby;
(d) Anyone charged with an offence is presumed innocent until proved guilty according to law;
(e) Anyone charged with an offence shall have the right to be tried in his presence;
(f) No one shall be compelled to testify against himself or to
confess guilt;

(g) Anyone charged with an offence shall have the right to examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(h) No one shall be prosecuted or punished by the same Party for an offence in respect of which a final judgment acquitting or convicting that person has been previously pronounced under the same law and judicial procedure;

(i) Anyone prosecuted for an offence shall have the right to have the judgment pronounced publicly; and

(j) A convicted person shall be advised on conviction of his judicial and other remedies and of the time-limits within which they may be exercised.

5. Women whose liberty has been restricted for reasons related to the armed conflict shall be held in quarters separated from men's quarters. They shall be under the immediate supervision of women. Nevertheless, in cases where families are detained or interned, they shall, whenever possible, be held in the same place and accommodated as family units.

6. Persons who are arrested, detained or interned for reasons related to the armed conflict shall enjoy the protection provided by this Article until their final release, repatriation or re-establishment, even after the end of the armed conflict.

7. In order to avoid any doubt concerning the prosecution and trial of persons accused of war crimes or crimes against humanity, the following principles shall apply:

(a) Persons who are accused of such crimes should be submitted for the purpose of prosecution and trial in accordance with the applicable rules of international law; and

(b) Any such persons who do not benefit from more favourable treatment under the Conventions or this Protocol shall be accorded the treatment provided by this Article, whether or not the crimes of which they are accused constitute grave breaches of the Conventions or of this Protocol.

8. No provision of this Article may be construed as limiting or infringing any other more favourable provision granting greater protection, under any applicable rules of international law, to persons covered by paragraph 1.

If such a regime had been in place over the last ten years, the option to capture and prosecute under an internationally recognized process would have given policy makers more choices. To a great extent, the recent changes to the military commissions rules have come very close to replicating the Article 75 guarantees. Covert actions that

47. Protocol I, supra note 12.
also have the option for capture and prosecution make the tool more nuanced and potentially more powerful in the struggle against violent extremism.

VIII. CONCLUSION

In summary, the modern battlefield, and the adaptive enemy therein, presents legal issues in deciding between covert action and traditional military activities. As a matter of law, the President may authorize any agency to conduct a covert action via presidential finding. Alternatively, the President must justify the use of force under traditional military activities under jus ad bellum doctrines in domestic and international law. While covert action has an important function in providing policymakers a precise tool to use in the spectrum between diplomatic and military force, legal bodies must use caution to ensure the “Fifth Function” is being used properly and not merely to circumvent legal requirements or media accountability. This accountability is especially important since it is politically easier for the executive branch to authorize covert action. This Article has also explored the idea of expanding covert action with the potential for capture and prosecution under an internationally recognized due process regime. Understanding this increasingly blurred line will not be easy, but if the general and statesman are to truly understand the nature of the war upon which they are embarking, an expanded covert action may function as a useful policy tool within the bounds of the law. In the end, as this Article has underscored, accountability married to the legitimacy of the rule of law is the core to a coherent grand strategy.

48. 50 U.S.C. § 413b(a), (e)(1)-(4).
49. CLAUSEWITZ, supra note 1.
ARTICLE

Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action

Andru E. Wall*

Abstract

Modern warfare requires close integration of military and intelligence forces. The Secretary of Defense possesses authorities under Title 10 and Title 50 and is best suited to lead US government operations against external unconventional and cyber threats. Titles 10 and 50 create mutually supporting, not mutually exclusive, authorities. Operations conducted under military command and control pursuant to a Secretary of Defense-issued execute order are military operations and not intelligence activities. Attempts by congressional overseers to redefine military preparatory operations as intelligence activities are legally and historically unsupportable. Congress should revise its antiquated oversight structure to reflect our integrated and interconnected world.

I. Introduction

After being hunted for nearly ten years, Osama Bin Laden was shot and killed by U.S. Navy SEALs in the early hours of May 2, 2011. The identity of the elite special operations unit that conducted the raid on bin Laden’s compound in Pakistan was not immediately released, as the

* Senior Associate with Alston & Bird LLP; former senior legal advisor for U.S. Special Operations Command Central (2007 to 2009). While this article was cleared for publication as required by my security clearance and nondisclosure agreements, the views expressed herein are my own and do not necessarily reflect the position of the U.S. government or Department of Defense. I thank Harvard Law School for its generous support of this paper and Jack Goldsmith, Hagan Scotten, Mark Grdovic, Nick Dotti, Chris Costa, Michael Bahar, and Lenn Ferrer for their invaluable comments and suggestions. To my beloved wife, Yashmin, and two adorable children, Isabella and Davi Alejandro, thank you for your extraordinary patience and support as I repeatedly disappeared to work on this article.
operation was described as covert. Yet as rumors swirled and information leaked to the media, Leon Panetta, the head of the Central Intelligence Agency (CIA) and soon-to-be-head of the Department of Defense (DoD), clarified during an interview that the operation to kill or capture bin Laden was a “Title 50” covert operation. Panetta explained that the raid was commanded by the President through Panetta, although “the real commander” was the head of Joint Special Operations Command, Vice Admiral William McRaven—the on-scene commander “actually in charge of the military operation that went in and got bin Laden.”

Panetta’s description of the bin Laden raid as a covert “Title 50” operation with a chain of command that included military commanders and the Director of Central Intelligence renewed a long-simmering debate within the national security community over “Title 10” and “Title 50” authorities. Titles 10 and 50 are part of the U.S. Code, but why would Panetta invoke a statute, the legal authority, to explain who was in charge of an operation conducted by military forces? We will see in a moment that the answer has everything to do with an antiquated congressional oversight paradigm and little to do with actual legal authorities.

The Title 10-Title 50 debate is the epitome of an ill-defined policy debate with imprecise terms and mystifying pronouncements. This is a debate, much in vogue among national security experts and military lawyers over the past twenty years, where one person gravely states “there are some real Title 10-Title 50 issues here,” others in the room nod affirmatively, and with furrowed brows all express agreement. Yet the terms of the debate are typically left undefined and mean different things to different people. If you

---

2 Admiral Vern Clark, former Chief of Naval Operations of the U.S. Navy, Professor John Radsan, a former assistant general counsel for the CIA, and Professor Gregory McNeal, a former Department of Justice lawyer, were asked “what is Title 10 authority?” and “what is Title 50 authority?” during a panel discussion at a law school symposium on national security law. Admiral Clark phrased the debate as one “about the line between covert and overt” (an issue we will examine in Part IV of this paper), yet his articulation of this concern focused on military transparency and public perceptions about the military. Professor Radsan framed the debate in terms of defined roles for the military and intelligence communities, while Professor McNeal opined that military lawyers advising special operations forces are often confused about the legal basis for their actions. National Security Symposium: The Battle Between Congress & The Courts in the Face of an Unprecedented Global Threat: Legislation Panel: Discussion & Commentary, 21 REGENT U.L. REV. 331, 347 (2009) [hereinafter “National Security Symposium”].
ask four military lawyers or DC policy wonks to define what "Title 10-Title 50 issues" means, you could get four different answers each cloaked in another layer of ambiguity, intrigue, and ignorance.

The Title 10-Title 50 debate is essentially a debate about the proper roles and missions of U.S. military forces and intelligence agencies. "Title 10" is used colloquially to refer to DoD and military operations, while "Title 50" refers to intelligence agencies, intelligence activities, and covert action. Concerns about appropriate roles and missions for the military and intelligence agencies, or the "Title 10-Title 50 issues" as commonly articulated, can be categorized into four broad categories: authorities, oversight, transparency, and "rice bowls." The first two concerns,

---

3 See, e.g., comments by James A. Lewis of the Center for Strategic and International Studies:

You have intelligence authorities, Title 50, and you have military authorities, Title 10. Well, what does the commander of Cyber Command do? Does he get to pick and choose between them? You need some way to say, "This kind of thing is military, you have to use the military decision chain," versus, "this kind of thing is intelligence, you have to use the intelligence decision chain." I'm not sure they've worked through all of that.


4 "Authorities" is a term commonly used by government lawyers and military personnel to describe statutory and delegated powers. For example, Title 10 of the U.S. Code created the Office of the Secretary of Defense and assigned the Secretary of Defense all "authority, direction and control" over DoD, including all subordinate agencies and commands. 10 U.S.C. § 113(b). Title 10 later created U.S. Special Operations Command (USSOCOM) and lists several tasks or missions that USSOCOM "shall be responsible for, and shall have the authority to conduct." 10 U.S.C. § 167. The President, in his role as Commander in Chief, may delegate through the Secretary of Defense additional responsibilities or "authorities" to USSOCOM, just as the Secretary of Defense may delegate certain of his statutory authorities to USSOCOM. These statutory and delegated responsibilities fall under the general rubric of "authorities." If the Commander of USSOCOM wants to conduct a given activity, he must first determine whether he possesses the statutory or delegated authority to use assigned personnel and resources to conduct the activity in question. Double-Tongued Dictionary defines "rice bowl" as: "in the military, a jealously protected program, project, department, or budget; a fiefdom. Etymological Note: Perhaps related to the Chinese concept of the rice bowl as a metaphor for the basic elements required to live, as seen, for example, in the iron rice bowl, empire that is guaranteed for life." Dictionary definition of "rice bowl", DOUBLE-TONGUED DICTIONARY,
authorities and oversight, are grounded in statutes and legislative history and are the focus of this article. The second two concerns, transparency and "rice bowls," can be quickly identified and dismissed as policy arguments rather than legitimate legal concerns.

Before delving into the law, we must first dismiss the policy arguments masquerading as Title 10-Title 50 issues. Transparency is the most amorphous concern in the Title 10-Title 50 debate. Often unacknowledged, the essence of this concern is the belief that intelligence operatives live in a dark and shadowy world, while military forces are the proverbial knights on white horses. Advocates of military transparency want to ensure the reputation of America's men and women in uniform remains un tarnished by association with the shadowy world of espionage. For these people, the Title 10-Title 50 debate is a debate about whether military forces should be engaged in "secret operations" or "go over to the dark side." Because secret

http://www.doubletongued.org/index.php/dictionary/rice_bowl (last visited Feb. 9, 2010). For an example of usage, see "Gingrich pledged 'to cooperate in any way I can on a bipartisan basis in really rethinking all of this' because the effort is 'going to require not only reshaping the rice bowls at the Pentagon but breaking a few of them.'" Fred Kaplan, In House, Bipartisan Drive is Growing to Slash Defense, BOSTON GLOBE, Jul. 29, 1990, at 2. See also "Attempting to take the moral high ground in a debate that in the past has been characterized by high emotions as each service sought to protect its own 'rice bowls.'" Army Seeks Moral High Ground In Briefing to Roles Panel, 184 DEFENSE DAILY 53 (Sept. 15, 1994).

5 The U.S. military consistently ranks at the apex of most-trusted institutions in the United States. This trust is critical to America's all-volunteer military and some even suggest the trust disparity between Congress and the military is one reason why Congress is loath to publicly attack military policies. David Hill, Respect for Military Surges, THE HILL (Jul. 18, 2006), http://thehill.com/opinion/columnists/david-hill/8251-respect-for-military-surges. A 2009 Gallop poll found 82% of Americans have a "great deal" or "quite a lot" of respect for the U.S. military, versus only 17% who felt the same way about Congress. Lydia Saad, Congress Ranks Last in Confidence in Institutions, GALLOP (July 22, 2010), http://www.gallup.com/poll/141512/congress-ranks-last-confidence-institutions.aspx.

6 In the words of Admiral Clark:

This line that exists [between covert and overt] is part of our good standing in the world. We have carefully tried to keep the military out of the covert world . . . . The covert side has appropriately resided within the CIA. We want the citizens, when they look at men and women wearing the cloth of the nation, to know that is who they are.

National Security Symposium, supra note 2, at 347.

7 "Secret operations" includes both covert and clandestine operations, which are terms this article will explore in greater detail in Parts III and IV. Professor Robin Williams argues "our cultural values do greatly affect our willingness as a nation to engage in
operations (used here in the colloquial sense that includes covert and clandestine operations) often require operating out of uniform, there are also concerns that military forces conducting such operations could lose protections under the Geneva Conventions (e.g., treatment as prisoners of war rather than as spies), increase risks to all U.S. military personnel serving abroad, and possibly endanger morale by sacrificing what is viewed as the moral high ground.\(^8\)

The second policy argument can be colloquially described as the “rice bowls” concern, which employs military jargon to describe those who jealously guard assigned programs, resources, and responsibilities.\(^9\) Bureaucrats jealously protect their “rice bowls” for two main reasons: to strengthen their position in the competition for scarce resources and to preserve their “lanes” or operational primacy in a given area. Broadly speaking, proponents of the “rice bowls” concern contend that Title 50 and Presidential orders make the CIA the lead U.S. agency for the collection of human intelligence\(^10\) and conduct of covert action, yet the military is unconventional warfare and do affect our policies and strategies in dealing with the widespread threats posed by infiltration and subversion on the part of hostile powers in many parts of the world.\(^\) Robin M. Williams Jr., *Are Americans and Their Cultural Values Adaptable to the Concept and Techniques of Unconventional Warfare?*, 341 ANNALS AM. ACAD. POL. & SOC. SCI. 82, 83 (1962), available at http://www.jstor.org/stable/1034146. Professor Williams suggests that “many Americans have come to think of unconventional warfare . . . in connection with the premeditated use of deception, subversion, and terror” and, thus, view unconventional warfare as incompatible with American values.


\(^9\) For a discussion of the term “rice bowls,” see supra note 4.

\(^10\) EXEC. ORDER No. 12,333, 46 Fed. Reg. 59941 (Dec. 4, 1981), amended by EXEC. ORDER No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008) [hereinafter E.O. 12,333], and 50 U.S.C. § 403-4a. During the Cold War, intelligence collection was organized by source and lead agency. The CIA was primarily responsible for human intelligence (HUMINT); the National Security Agency (NSA) was primarily responsible for signals intelligence (SIGINT); and the National Geospatial Intelligence Agency was primarily responsible for overhead imagery intelligence (IMINT). As one intelligence expert explains: “There was, perhaps, a certain logic to that organization during the Cold War. With one overwhelming target—the Soviet Union—the various “INTs” were asked, in effect, what they could contribute to understanding the puzzle of the Soviet Union.” GREGORY F. TREVERTON, INTELLIGENCE FOR AN AGE OF TERROR 6 (2009). Treverton points out that on the analytic side, this organization permitted competition, of sorts, as the CIA focused on the national and political aspects of intelligence, while the Defense Intelligence Agency and service intelligence elements “naturally focused more on military dimensions of problems that cut across the military and political.” Id. at 50. There is an ongoing debate over whether
stealing from the CIA’s “rice bowl” by expanding its human intelligence capabilities under the guise of Title 10 authorities. The belief is that this expansion by the military threatens to divert resources from the CIA and could lead to operational deconfliction issues.11 For the CIA and its Congressional proponents, the concern is that the CIA’s legal role as lead agency is diminished as it is dwarfed in size by the military’s rapidly expanding human intelligence capabilities.12 When budgets shrink and resources are scarce, the fear is the CIA will be disproportionately impacted.

The related rice bowls concern of “lanes” raises actual operational issues. If the military’s human intelligence collection resources dramatically exceed the CIA’s resources, the CIA may find it difficult to execute its statutory role as lead agency for the coordination and deconfliction of U.S. government human intelligence collection.13 A few hundred CIA officers may find it impossible to coordinate and deconflict the human intelligence activities conducted by thousands of military personnel, thereby de facto ceding the CIA’s statutory primacy.14 In a worst-case scenario, the failure to organizing intelligence collection in this manner remains appropriate to respond to the threats of the 21st century.

11 To those on the CIA’s side, human intelligence collection efforts would see “a quantum improvement in capability” if “lanes” across the intelligence community were enforced. John MacGaffin, Clandestine Human Intelligence: Spies, Counterspies, and Covert Action, in TRANSFORMING U.S. INTELLIGENCE 79, 91 (Jennifer E. Sims & Burton Gerber, eds., 2005). The term “deconfliction” is commonly used in military and intelligence circles to refer to processes or coordination intended to ensure that various operations or activities do not interfere with each other.


13 During confirmation hearings for General Michael Hayden after he was nominated in 2006 to become Director of the CIA, Senator Olympia Snowe opined that as the military seeks to “further expand and encroach in areas . . . [such as] clandestine forces, paying informants, gathering deeper and deeper into human intelligence, I think that this is going to be a serious—potentially—contest if the CIA does not regain its ground and reclaim its lost territory.” Nomination of General Michael V. Hayden, USAF to be Director of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence, 109th Cong., 2nd Sess. 50 (2006) [hereinafter Hayden Nomination].

14 The DoD controls about 80% of the intelligence budget, which presumably only includes DoD agencies that are also part of the intelligence community; most of the 80% is spent on
maintain clear operational lanes could lead to operatives unintentionally impeding or even exposing each other’s human intelligence efforts. The salient point, however, is not that the military is exceeding its statutory authority, but rather that both the military and intelligence agencies possess the statutory authority to conduct intelligence-gathering activities that may be indistinguishable “to the naked eye.” This is a valid operational concern and unremitting management challenge; intelligence agencies must strive to ensure the military’s intelligence collection activities are coordinated, deconflicted, and conducted according to established standards.

None of these concerns suggest that a certain activity (or method of conducting that activity) is inconsistent with statutory or legal authority; rather, each suggests that a certain activity ought not to be conducted (or ought to be conducted) a certain way because of practical effects. Guarding the U.S. military’s reputation and protecting an agency’s resources are legitimate policy considerations, just as preserving lanes and ensuring deconfliction is a crucial operational concern. Yet it is misleading to couch these policy and operational debates in terms of statutory law, and it is misleading to label these concerns as “Title 10-Title 50” issues. Transparency, rice bowls and lanes are concerns that can be adequately addressed by sound Executive Branch management and proper allocation of resources by Congress.

Having defined the Title 10-Title 50 debate and summarily exposed the policy arguments and operational challenges that often masquerade as legal issues, this article now turns in Part II to analyzing the significant legal authorities given to the President and Secretary of Defense under the U.S. Constitution and Titles 10 and 50 of the U.S. Code. That “Title 10” is commonly used to refer to DoD and to articulate the legal basis for military operations is understandable. However, the use of “Title 50” to refer solely to activities conducted by the CIA is, at best, inaccurate as the Secretary of Defense also possesses significant authorities under Title 50.


15 General Hayden correctly noted “that what DoD is doing under title 10 authorities and what CIA does under title 50 may be indistinguishable to the naked eye . . . get kind of merged so that the actions are actually on the ground, in reality indistinguishable, even though their sources of tasking and sources of authority come from different places.” Hayden Nomination, supra note 13, at 50–51.
After establishing the relevant legal authorities, Part III discusses Congressional oversight, which reveals itself as the true Title 10-Title 50 issue. It is Congress's antiquated oversight structure and a concomitant misunderstanding of the law that casts a shadow of concern and purported illegitimacy over military operations that resemble activities conducted by intelligence agencies. Congress's stovepiped view of national security operations is legally incongruous and operationally dangerous because it suggests statutory authorities are mutually exclusive and it creates concerns about interagency cooperation at exactly the time in history when our policy and legal structures should be encouraging increased interagency coordination and cooperation against interconnected national security threats.

Concern over purported Title 10-Title 50 issues arises most often in the context of discussions over unconventional and cyber warfare. While most details of how these operations are conducted are not publicly available, Part IV will define unconventional warfare and cyberwarfare and generally explain their purpose, role, and conduct. These military operations are conducted in secret and in environments where public acknowledgement of the U.S. military's involvement may raise diplomatic and national security concerns (e.g., other countries and cyberspace), which is why Congressional intelligence committees often mistakenly conclude they should have oversight of these military operations. However, when the law (and even Congress's own legislative history) is applied to unconventional warfare and cyberwarfare in Part IV, it becomes apparent that these are military operations rather than intelligence activities so long as they remain under the command and control of a military commander and are conducted prior to or during (anticipated or actual) acknowledged military operations. Part V offers a few concluding thoughts and recommendations.

II. The Law Permits While Congress Attempts to Restrict

The Title 10-Title 50 debate is typically invoked to express concerns that the military is taking over missions and activities "properly" within the sole domain of the intelligence agencies. While ordinary Americans in the heartland may care only that U.S. national security objectives are effectively accomplished, military and intelligence bureaucrats and their Congressional overseers remain obsessed with who actually does the mission. Yet a careful
analysis of the law and related legislative history shows how the law permits much of what Congress attempts to restrict with its stovepiped approach to oversight of the military and intelligence community.

A. Legal Authorities

Professor Gregory McNeal, sitting on a law school panel discussing Title 10—Title 50 issues, suggested that lawyers advising special operations units may have trouble discerning whether they are operating under Title 10 or Title 50 authorities. McNeal elaborated:

When the military goes out, there are JAGs who sit with intelligence agents or officials and advise on whether it is lawful to strike a specific target or engage in a specific operation. If a JAG is seated in a targeting cell in a special operations unit, the first question will still be whether a certain target can be attacked. However, the second question that the officer in that cell will oftentimes ask is whether he is operating under Title 10 or Title 50 authority. If it is a CIA drone, the answer may be that it is fine to hit the target. Under Title 10 the answer may be, no you cannot.

Professor McNeal’s hypothetical evidences a misunderstanding or mischaracterization of the law and conduct of military operations. Military personnel, including Professor McNeal’s hypothetical “special operations unit,” operate under military direction and control and under Title 10 authority. CIA personnel operating under a CIA direction and control operate under Title 50 authority. CIA personnel operating with military personnel may use their Title 50 authorities to support a Title 10 operation, but they would still be operating under Title 50 authority; likewise, a

---

16 National Security Symposium, supra note 2, at 348–49.
17 Id. at 349.
18 Professor McNeal may be confusing or merging statutory authority with delegated authorities such as rules of engagement (ROE). For example, in the hypothetical McNeal presents, it is theoretically possible that the CIA drone (operating under Title 50 authority in support of a Title 10 military operation) may be operating under different ROE than the special operations unit it is supporting. The CIA rules of engagement may provide that a target can be attacked if X+Y exists, while the military ROE may require X+Y+Z, i.e. the CIA ROE may be more or less permissive than the military ROE. But rules of engagement are policy directives, not statutes, so their characterization as a “Title 10” or “Title 50” issue is inaccurate and misleading.
military unit operating under Title 10 authority could support a Title 50 operation (if they are given such delegated authority). In other words, when an operation is termed a "Title 10" operation, that statutory label simply refers to the statutory origins of the mission commander's authority; this does not preclude other government agencies operating under separate statutory authorities from using their personnel and resources to support the "Title 10" operation.

1. The President's Constitutional Authority

Our analysis of legal authorities possessed by military commanders begins with the executive and commander-in-chief powers, delineated in the U.S. Constitution and applicable federal statutes, and delegated from the President through the Secretary of Defense down to subordinate commanders. Delegated authorities derive from a myriad of Executive Branch policy documents, including directives issued by various echelons within DoD. As the overwhelming majority of directives relating to unconventional and cyber warfare are classified, our discussion here will focus on the statutes: policy may restrict statutory authorities, but policy can also be changed at the President's direction. While the majority of national security decisions are made on a daily basis pursuant to statutory and delegated authority, there is no question that the President is the head of the executive branch and commander in chief.20

The President's authority to direct military operations and intelligence activities against external threats resides in his Constitutional executive and commander-in-chief powers.21 The President is vested with

---

19 Challenges do arise when special operations forces (SOF) operate with CIA personnel, as happened in Afghanistan in late 2001 and in Iraq in early 2003. Operators may ask when tasked with a particular mission: "am I conducting this mission under Title 10 or Title 50 authorities?" The question, however, is generally one of fiscal authorities rather than operational authorities. Are CIA funds or DoD funds being used to pay for the operation? If the CIA is paying a particular Northern Alliance commander to employ his forces in furtherance of U.S. military objectives, is that a Title 10 activity or a Title 50 activity? Can SOF employ indigenous forces trained and equipped by the CIA under Title 50 authorities in furtherance of SOF's Title 10 missions? These are important questions that require close examination of the relevant operational orders and fiscal authorities.


21 The President is vested with executive power by Article II, Section 1 of the U.S. Constitution; Section 2 adds commander-in-chief powers.
executive power\textsuperscript{22} and is the "sole organ of the federal government in the field of international relations—a power which does not require as a basis for its exercise an act of Congress."\textsuperscript{23} As chief executive, the President may "manage the business of intelligence in such a manner as prudence may dictate."\textsuperscript{24} This includes the authority to secretly collect intelligence for reasons of national security.\textsuperscript{25} As commander in chief, the President may employ the military to protect the national interests of the United States as he deems necessary.\textsuperscript{26}

The President does not wield these powers exclusively, however, as Congress is given the authority to "raise and support Armies," to "provide and maintain a Navy," to appropriate funds to support the military, and to issue formal declarations of war.\textsuperscript{27} Simply put, Congress decides how to resource the U.S. military and when to formally declare war, while the President decides how to employ the military in furtherance of U.S. national security objectives—subject always to constitutionally permissive constraints enacted by Congress and available funding.

Perhaps the most significant restraint, or attempted restraint, upon Presidential employment of the military is contained in the War Powers Resolution of 1973, which directs the President to notify Congress within 48-hours after deploying military forces in situations where hostilities are

\textsuperscript{22} U.S. CONST. art. II, § 1.
\textsuperscript{23} United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936). Note, however, that "sole" does not mean the Supreme Court will not on rare occasions conduct its own inquiry to ensure that Presidential assertions that particular actions are grounded in these powers, are so in fact. In Youngstown, President Truman contended that his Constitutional commander-in-chief authorities permitted the seizure of steel mills in the United States, but the Supreme Court held: "we cannot with faithfulness to our constitutional system hold that the Commander in Chief of the Armed Forces has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production." Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 587 (1952).
\textsuperscript{24} THE FEDERALIST No. 64 (John Jay).
\textsuperscript{25} See, e.g., Chicago & S. Air Lines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948); Toten v. United States, 92 U.S. 105, 106 (1876) (The President "was undoubtedly authorized during the war, as commander-in-chief, to employ secret agents to enter rebel lines and obtain information respecting the strengths, resources, and movements of the enemy.").
\textsuperscript{26} In the Prize Cases, the U.S. Supreme Court held that determinations of belligerency and threats to national security are questions to be decided by the President. Prize Cases, 67 U.S. 635, 670 (1863).
\textsuperscript{27} U.S. CONST. art. I, § 8, cl. 1 & 11–13.
anticipated. The President must generally withdraw the military forces within sixty days unless Congress formally declares war or otherwise authorizes the combat deployment. The War Powers Resolution was passed over President Richard Nixon’s veto, and every subsequent President has also believed that “the War Powers Resolution is an unconstitutional infringement by the Congress on the President’s authority as Commander-in-Chief.”

This Constitutional separation or balancing of power between the President and Congress with respect to war powers sparked intense debate nearly as soon as the Constitution was ratified. Discussions of the President’s constitutional authority as commander in chief implicate “some of the most difficult, unresolved, and contested issues in constitutional law.” This debate is perhaps best pictured as a Venn diagram: some assert a circle of “inherent” Presidential power, some favor a circle of Congressional checks on “imperial” Presidential power, while others see a Constitutional overlap or balancing of powers between the two branches. One scholar astutely observes that “[w]riters on the relative powers of the presidency versus the Congress almost invariably lapse into advocacy when they comment on the textual, historical or functional bases of war powers.”

Those who favor presidential powers in the realm of national security point to the President’s enumerated powers, namely the “executive

29 Two key provisions of the War Powers Resolution link the President’s authority to deploy military forces for reason of national security with Congress’s power of the purse: the President must notify Congress when troops are deployed equipped for combat, 50 U.S.C. § 1543(a)(1), after which Congress has sixty days to authorize the deployment or the President must terminate the use of force. 50 U.S.C. § 1544(b).
30 CONGRESSIONAL RESEARCH SERVICE, WAR POWERS RESOLUTION: PRESIDENTIAL COMPLIANCE 2 (2002). It is worth noting that President Nixon’s veto centered on two Constitutional concerns: the provision under which funding would be automatically cut off if Congress fails to act within 60–90 days after Presidential notification (§ 1544(b)), and the provision permitting Congress to direct cessation of the deployment by passage of a mere concurrent resolution, which normally does not have power of law. President Nixon believed that only an affirmative act of Congress could override the President’s decision to deploy military forces under his Commander-in-Chief authority. Letter from President Richard M. Nixon to the House of Representatives, Veto of the War Powers Resolution (Oct. 24, 1973), available at http://www.presidency.ucsb.edu/ws/index.php?pid=4021.
32 Michael Bahar, Axes of Power: Predicting the Reception of Assertions of Presidential War Powers In the Courts, 58 NAVAL L. REV. 1, 1 (2009).
Power” of Article II, section 1 and the “Commander in Chief” power of Article II, section 2. They assert the only constitutional limitations on those powers are Congress’s power of the purse and power to formally declare war.33 In other words, in situations where a declaration of war is not required (e.g., self-defense or peacetime intelligence activities), the only way Congress can impede Presidential power is by cutting off funding.

Advocates of Congressional war powers, however, argue against rigid interpretations of the Constitutional text and quote James Madison and other framers of the Constitution at length to support their vision of a “national security Constitution” where “Congress, the courts, and the Executive should interact in the foreign policy process.”34 These advocates argue that “[t]he constitutional framework adopted by the Framers is clear in its basic principles. The authority to initiate war lay with Congress. The President could act unilaterally only in one area: to repel sudden attacks.”35

While reviewing two diametrically opposed books on Presidential war powers, Professor Jack Goldsmith succinctly summarizes the intellectual history of arguments debating Presidential and Congressional war powers before wryly observing “that constitutional theory is usually grounded in a theory of preferred outcomes.”36 Presidential power has grown of necessity beyond what the framers could have imagined, yet meaningful Congressional checks on Presidential power remain and “translate, in a


35 Fisher, supra note 34, at 11.

rough way, the Framers’ original design.” Goldsmith concludes: “the larger picture is one that preserves the original idea of a balanced constitution with an executive branch that remains legally accountable despite its enormous power.”

2. The Secretary of Defense’s Statutory Authorities

Congress modernized and reorganized the U.S. national security establishment in the National Security Act of 1947. The act merged the War and Navy departments into the DoD, and created the National Security Council, CIA, National Security Agency (NSA), and other agencies. The Act also established a formalized process for national security decision-making and Congressional oversight of intelligence activities. The National Security Act of 1947, as amended, is found in Title 50 of the U.S. Code.

In 1956 and 1962, Congress removed from Title 50 provisions relating to organization and functions of the services and DoD and placed these provisions with amendments in Title 10 of the U.S. Code. In 1986, following the failed Iran hostage rescue mission, Congress legislated a new “joint” structure of command and control through which the President exercises his commander-in-chief responsibilities.

The President exercises Constitutional authority as Commander in Chief through the Secretary of Defense who is also his “principal assistant . . . in all matters relating to the Department of Defense.” Title 10 gives the Secretary of Defense all “authority, direction and control” over DoD, including all subordinate agencies and commands. Title 10 also created combatant commands, which include geographic commands (e.g., U.S.

37 Id.
38 Id.
41 10 U.S.C. §§ 101–18505. Laws pertaining to the National Guard were transferred to Title 32.
43 10 U.S.C. § 113(b) (2006). Title 10 specifically states that DoD is part of the executive branch, which removes any doubt about the President’s authority over the department under both section 1 (executive power) and section 2 (Commander-in-Chief power) of Article II of the U.S. Constitution. See 10 U.S.C. § 111 (2006).
European Command) and U.S. Special Operations Command (USSOCOM). Title 10 gives combatant commands statutory authorities and their commanders report directly to the Secretary of Defense.\textsuperscript{45} For example, Title 10 gives USSOCOM authority over the following activities when conducted by special operations forces: direct action, strategic reconnaissance, unconventional warfare, foreign internal defense, civil affairs, psychological operations, counterterrorism, humanitarian assistance, theater search and rescue, and such other activities as may be specified by the President or the Secretary of Defense.\textsuperscript{46}

Title 50 establishes, defines and delineates authorities within the intelligence community, but it also clarifies that the Secretary of Defense controls those members of the U.S. intelligence community, such as the NSA and Defense Intelligence Agency, that are part of DoD.\textsuperscript{47} The Secretary of Defense's control and direction of DoD human intelligence activities can be limited only by the President.\textsuperscript{48} This provision is reinforced by Title 10, which creates an Undersecretary of Defense for Intelligence to whom the Secretary of Defense may delegate duties and powers “in the area of intelligence.”\textsuperscript{49} Finally, Executive Order 12,333, which has regulated the U.S. intelligence community for nearly thirty years, directs the Secretary of Defense to “[c]ollect (including through clandestine means), analyze, produce, and disseminate information and intelligence [as well as] . . . defense and defense-related intelligence and counterintelligence . . . .”\textsuperscript{50}

One source of confusion in the Title 10-Title 50 debate springs from Title 50's use of the term “national intelligence.” The discussion of “national intelligence” in Title 50 causes some to opine that “national intelligence” is separate and distinguishable from military intelligence,\textsuperscript{51} yet

\textsuperscript{45} 10 U.S.C. §§ 161, 162, 164, 165, 166, 166a, 166b, & 168 (2006). In practice, the combatant commanders communicate with the Secretary of Defense via the Joint Staff. Although the Chairman of the Joint Chiefs of Staff is not technically or legally in the chain-of-command, his statutory role is that of advisor to the President and Secretary of Defense. The Chairman of the Joint Chiefs of Staff has a staff of several thousand personnel, the Joint Staff, through which all operational orders and communications to and from the Secretary of Defense flow.


\textsuperscript{48} \textit{Id.} at § 403–5(b)(5) (2006). \textit{See also supra} note 10.


\textsuperscript{50} E.O. 12,333, supra note 10, at ¶1.10.

\textsuperscript{51} \textit{See} 50 U.S.C. §401a(5) (2006). Intelligence activities are further stove-piped. Following the passage of the National Security Act of 1947 and continuing through the end of the
other provisions of Title 50 include references to the intelligence needs of combatant commanders, tactical intelligence activities, and the intelligence needs of the military's operational forces. These terms, read in the context of Title 50, suggest labels based on the intended primary consumer of the intelligence, or its primary purpose, not an attempt to categorize or label intelligence by type or the agency collecting the intelligence.

There is no rigid separation between Title 10 and Title 50. A more accurate interpretation is simply that Title 10 clarifies roles and responsibilities within DoD, while Title 50 clarifies roles and responsibilities within the intelligence community; both titles explicitly recognize that the Secretary of Defense has statutory roles and authorities under Title 10 and under Title 50. Executive Order 12,333 confirms this reading by directing the Secretary of Defense to collect intelligence for both his department and the intelligence community writ large. U.S. military doctrine further erodes any attempted distinction between tactical, operational, and strategic intelligence:

National assets such as intelligence and communications satellites, previously considered principally in a strategic context, are an important adjunct to tactical operations. Actions can be defined as strategic, operational, or tactical based on their effect or contribution to achieving strategic, operational, or tactical objectives, but many times the accuracy of these labels can only be determined during historical studies.

Read in concert with Title 10, Title 50 does not infringe upon the Secretary of Defense's authorities to collect intelligence. Rather, Title 50 recognizes the authorities assigned to the Secretary of Defense under Title 10 over all

Cold War, the U.S. national security establishment maintained a distinction between military or tactical intelligence and national or foreign intelligence. In the context of the Cold War, this distinction made sense. Domestic, foreign, and military intelligence were three separate categories with separate legal authorities and executing agencies. The Director of Central Intelligence leads and directs national intelligence collection activities under authorities found in Title 50. The Intelligence Community components of DoD often collected foreign intelligence in response to national tasking under Title 50 authorities, but they also collected tactical intelligence for military commanders.

DoD intelligence activities, and adds Title 50’s provisions regarding Congressional oversight to intelligence activities conducted primarily by DoD personnel in support of or in furtherance of tasking from the Director of National Intelligence (DNI) (as opposed to tasking from the Secretary of Defense).

Thus, Title 10 and Title 50 are mutually-reinforcing authorities, not mutually-exclusive authorities; these statutory authorities may even be exercised simultaneously by personnel under the command and control of the Secretary of Defense. Labeling some intelligence activities “Title 50” activities while labeling similar activities “Title 10” activities creates a distinction where the law does not. Importantly, the statutes make distinctions based on direction, control, and funding—not on nomenclature.

B. Congressional Oversight

Confusion over Title 10 and Title 50 authorities has more to do with congressional oversight and its attendant internecine power struggles than with operational or statutory authorities. Operators, be they special operations forces (SOF) operating under Title 10, CIA agents operating under Title 50, or NSA personnel operating under both Title 10 and Title 50, know from whence their authorities are derived. The operators recognize dual lines of authority and are primarily concerned with coordination and deconfliction. To outsiders looking in, such as a Senator in Washington, DC, the activities performed by SOF and CIA operatives, especially during periods preceding possible or anticipated conflict, may appear virtually indistinguishable. Yet similarity in no way vitiates their dual lines of authority, nor does it create great challenges for operators.

A former general counsel of the CIA, Jeffrey H. Smith, spoke of what he perceived as a “dichotomy between Title 10 and Title 50” that gives “executive branch lawyers and members of Congress . . . headaches.”54 These headaches arise, Smith stated, during debates over military activities called “preparation of the battlefield,” which are activities typically carried out by military personnel “in close collaboration with the

---

U.S. intelligence community. 55 We will examine these activities more closely in Parts III and IV. Smith, however, summarizes the issue as such: if the activity is defined as a military activity ("Title 10") there is no requirement to notify Congress, while intelligence community activities ("Title 50") require presidential findings and notice to Congress. 56 The natural inclination for executive branch lawyers, according to Smith, is to prefer the Title 10 paradigm to obviate congressional notification requirements. 57

This perception—that the Executive Branch is deliberately trying to avoid congressional oversight—naturally riles the intelligence committees. In its report accompanying the Intelligence Authorization Act for Fiscal Year 2010, the House Permanent Select Committee on Intelligence noted "with concern the blurred distinction between the intelligence-gathering activities carried out by the Central Intelligence Agency (CIA) and the clandestine operations of the Department of Defense." 58 The Committee accused DoD of labeling its clandestine activities as operational preparation of the environment (OPE) in order to justify them under Title 10 and avoid oversight by the intelligence committees "and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction. 59 The Intelligence Committee apparently perceives an oversight lacuna, yet no such lacuna exists. Rather, all activities conducted under Title 10 authorities are subject to oversight by the armed services committees and, for example, commanders of special operations forces regularly brief the armed services committees on their clandestine activities.

55 Id. at 546.
56 Smith considers it "a curiosity of our legal history that findings and notice to Congress are required even in the most minor of covert actions, whereas no such requirement governs the use of our military forces." Id. Others express a similar envy of what they perceive to be DoD's easier operations approval process: "When the CIA acts, it requires a presidential 'finding' sent to Congress; yet the military can be authorized simply through the chain of command from the president as commander in chief." TREVERTON, supra note 10, at 13.
57 Smith, supra note 54, at 547.
59 Id.
Figure 1: Congressional Oversight of Intelligence Activities and Military Operations

As illustrated by Figure 1, the congressional intelligence committees exercise oversight of intelligence activities, while the armed services committees exercise oversight jurisdiction over military operations. The congressional oversight is not coterminous with statutory authorities, as Title 10 includes authority for the Secretary of Defense to engage in both intelligence activities and military operations. Congressional oversight overlaps when non-DoD elements of the intelligence community provide support to military operations and in the unlikely or at least rare instance where the President directs elements of DoD to conduct covert action.

---

60 Senate Select Committee on Intelligence (SSCI); House Permanent Select Committee on Intelligence (HPSCI); Senate Armed Services Committee (SASC); and House Armed Services Committee (HASC).

61 "No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law
Oversight would also overlap with respect to intelligence activities carried out by an element of the intelligence community in support of a military operation authorized under Title 10.

Congressional oversight of the military is straightforward: both the Senate and House Armed Services Committees exercise jurisdiction over all aspects of DoD and matters relating to "the common defense." Defense authorization bills originate in the armed services committees, where they must be approved before consideration by the full Senate or House. Problems arose in the wake of 9/11 as DoD expanded its intelligence capabilities in order to support ongoing military operations, and the intelligence committees correspondingly sought to expand their jurisdiction in an attempt to bring all military intelligence collection efforts within their purview, which created clashes with the armed services committees and the Executive Branch and generated debates over appropriate congressional oversight.

Congressional oversight of intelligence activities is considerably more complex. The National Security Act of 1947, which created the CIA, did not include statutory congressional oversight provisions. For nearly thirty years, Congress exercised little oversight of intelligence activities. This changed dramatically, however, following revelations in 1974 by then New York Times reporter Seymour Hersh that U.S. intelligence agencies engaged in domestic spying. The Church Committee's subsequent investigation "did nothing less than revolutionize America's attitudes toward intelligence supervision."

The Senate established its Select Committee on Intelligence (SSCI) in 1976 and the House followed suit a year later with its Permanent Select Committee on Intelligence (HPSCI). The era of benign neglect was over, replaced instead by dynamic if often dysfunctional congressional oversight. In 1980 Congress mandated for the first time that the Director of Central

---

93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective." E.O. 12,333, supra note 10, at ¶ 1.7(a)(4).

62 S. COMM. ON RULES AND ADMIN., 111TH CONG., STANDING RULES OF THE SENATE R. XXV, 1(c)(1) (2009) [hereinafter SENATE RULES]; RULES OF THE HOUSE OF REPRESENTATIVES (111th Cong.) Rule X, 1(c) [hereinafter HOUSE RULES].


64 Id. at 199.
Intelligence and the heads of all other U.S. departments and agencies "involved in intelligence activities" keep the intelligence committees "fully and currently informed of all intelligence activities."\(^{65}\) This provision was repealed in 1991 and responsibility for informing the congressional intelligence committees of all intelligence activities, including anticipated activities, was placed directly on the President.\(^{66}\)

The intelligence committees exercise broad oversight of the intelligence community. They exercise exclusive authorizing powers for the CIA, the Director of National Intelligence, and the National Intelligence Program.\(^{67}\) They share jurisdiction of DoD intelligence components with the Senate and House armed services committees.

While the jurisdictions of the Senate and House intelligence committees are nearly identical, HPSCI exercises broader jurisdiction in two significant respects: HPSCI uses a much broader definition of intelligence activities and adds oversight of "sources and methods."\(^{68}\) SSCI

---

\(^{65}\) Intelligence Authorization Act for 1981, 94 Stat. 1981, Pub. L. 96-450 (1980), repealed by Intelligence Authorization Act for 1992, 105 Stat. 441, Pub. L. 102-88 (1991). While a detailed examination of the Constitutional permissibility of this statute is beyond the scope of this essay, it is worth noting that this provision was prefaced with the following caveat: "To the extent consistent with all applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches of the Government."


\(^{67}\) The National Intelligence Program is defined as:

> All programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.


\(^{68}\) Authority to "review and study on an exclusive basis the sources and methods of entities" in the intelligence community was added in January 2001. House Rule 3(l), added by
exercises jurisdiction over “intelligence activities,” while HPSCI exercises jurisdiction more broadly over “intelligence and intelligence-related activities . . . including the tactical intelligence and intelligence-related activities of the Department of Defense.”

The House gives “intelligence and intelligence-related activities” this all-encompassing definition:

[The] collection, analysis, production, dissemination, or use of information that relates to a foreign country, or a government, political group, party, military force, movement, or other association in a foreign country, and that relates to the defense, foreign policy, national security, or related policies of the United States and other activity in support of the collection, analysis, production, dissemination, or use of such information.

Thus, the House of Representatives via a rule change gave HPSCI oversight of “intelligence-related activities” including “tactical intelligence” and other military information collection activities for which congressional notification is not statutorily mandated. This would be understandable if HPSCI controlled authorizations for those military activities, but it does not. All authorizations for these military activities originate in the House Armed Services Committee and House rules do not provide for their review by the intelligence committee. In fact, just the opposite occurs as all intelligence authorization bills passed by the intelligence committees must then clear the armed services committees before being considered by the full House.

Intelligence committee oversight is weakened by the bifurcated authorization and appropriations processes. Because most appropriations for intelligence activities are included as a classified section of the annual defense appropriations bill, “the real control over the intelligence purse lies

H.Res. 5, 107th Cong. (Jan. 3, 2001). Sources and methods is a catch-all phrase used by the intelligence community that eludes to how and from whom information is gathered.


70 Id. at Rule X, 111(j)(1). This definition applies to covert and clandestine activities. Title 50 does not define “intelligence activities,” although it does state that the term “includes covert actions . . . and includes financial intelligence activities.” Section 413a of Title 50 sets forth a generalized reporting requirement for intelligence activities other than covert actions, while Section 413b delineates detailed reporting and Presidential approval requirements for covert actions (“findings”). Executive Order 12,333 defines intelligence activities as “all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.” E.O. 12,333, supra note 10.
with the defense subcommittees of the House and Senate Appropriations Committees.”71 The 9/11 Commission recognized how “dysfunctional” this arrangement is in practice and recommended the establishment of a single joint intelligence committee with authorizing and appropriating authorities.72 Congress, to its detriment, has not adopted this recommendation.

Intelligence committee oversight is further weakened by the failure to enact an intelligence authorization bill for five of the past six years. Title 50 prohibits the expenditure or obligation of appropriated funds on intelligence or intelligence-related activities unless “these funds were specifically authorized by Congress for such activities.”73 Congress meets this “specifically authorized” provision through the use of a catch-all provision inserted into the defense appropriations acts.74 Over the past 30 years, Congress enacted an intelligence authorization bill prior to the start of the fiscal year on just two occasions—1983 and 1989.

Congress could end the Title 10-Title 50 debate by simply reforming its oversight of military and intelligence activities and align oversight with the statutory authorities. Rather than focus on what the activity in question looks like (what is being done), Congress should simply ask who is funding the activity and who is exercising direction and control; oversight should be aligned in the House and Senate and should correspond to funding,

71 Jennifer Kibbe, Congressional Oversight of Intelligence: Is the Solution Part of the Problem?, 25 INTELLIGENCE AND NAT’L SECURITY 24–49, 29–30 (2010). This process protects national security by sheltering intelligence budgets from public view, but it also dilutes the role of the intelligence committees. Kibbe points out that “the structure of the system precludes the defense subcommittees from conducting stringent intelligence oversight . . . [as] the $75 billion intelligence budget comprises around 10 to 12 percent of the defense budget” and, thus, garners “very little attention.”
74 The catch-all provisions read similar to this one for fiscal year 2009:

Funds appropriated by this Act, or made available by the transfer of funds in this Act, for intelligence activities are deemed to be specifically authorized by Congress for the purposes of section 504 of the National Security Act of 1947 (50 U.S.C. 414) during fiscal year 2009 until enactment of the Intelligence Authorization Act for Fiscal Year 2009.

direction and control. Congress should adopt the recommendations of the 9/11 Commission—align congressional oversight with statutory authorities and reform its bifurcated intelligence authorization and appropriations functions—and thereby eliminate most real and perceived Title 10-Title 50 issues. With the crux of the Title 10-Title 50 debate exposed as dysfunctional congressional oversight, this article now turns to explaining why some military and intelligence activities look alike, yet remain distinguishable.

III. When Military Operations Look Like Intelligence Activities

When American forces entered Afghanistan shortly after the terrorist attacks of 9/11, the picture soon emerged of U.S. Army Special Forces ("Green Berets") and CIA paramilitary officers operating together with Afghan warlords against a common al Qaeda and Taliban enemy. Presidential approval of the unconventional warfare plan for Afghanistan did much to quell rumblings about blurring of military and intelligence authorities, yet as the war in Afghanistan continued and the "war on terror" expanded globally those concerns became more prominent. Some argued the "tight integration" between special operations forces and the CIA in Afghanistan signaled "the erosion of distinctions between SOF and the CIA"—an "erosion" with supposedly dire legal consequences.

A former general counsel for the CIA suggested an erosion of distinctions between military operations and covert action in the context of cyberwarfare. John Rizzo characterized the Title 10-Title 50 debate in

---


76 COLONEL KATHRYN STONE, "ALL NECESSARY MEANS"—EMPLOYING CIA OPERATIVES IN A WARFIGHTING ROLE ALONGSIDE SPECIAL OPERATIONS FORCES 4 (US ARMY WAR COLLEGE STRATEGY RESEARCH PROJECT) (2003).

77 Hiding our Cyberwar from Congress, EMPTYWHEEL (Jan. 14, 2011), http://emptywheel.ireddoglake.com/2011/01/14/hiding-our-cyberwar-from-congress (last accessed Mar. 9, 2011). This blogger provides three examples to support the thesis that DoD is deliberately trying to avoid reporting information on cyberwarfare programs to Congress. The third example quotes from a speech delivered by John Rizzo, former general counsel of the CIA, to the American Bar Association's Standing Committee on National Security. Rizzo stated: "I've always found fascinating and personally I think it's a key to understanding many of the legal and political complexities of so-called cyberlaw and cyberwarfare is the division between Title 10 operations and Title 50 operations. Title 10
terms of a dichotomy between “war-making authority” and “covert action” before concluding that “how these cyber-operations are described will dictate how they are reviewed and approved in the executive branch, and how they will be reported to Congress, and how Congress will oversee these activities.” Some commentators used Rizzo’s observation to suggest that the executive branch was disingenuously describing cyberwarfare in attempt to evade congressional oversight. We saw in Part II that oversight by the armed services committees is still congressional oversight. Part III will now explain why the same activities can properly be described as military or intelligence activities depending on their command and control, as well as funding, context and mission intent.

A. Unconventional Warfare

Just eight days after the terrorist attacks of September 11, 2001, Gary Schroen, a CIA paramilitary officer, packed three boxes with $9 million and flew to Afghanistan. The money would be used to pay Afghan warlords to fight with CIA and Special Forces personnel against al Qaeda and its Taliban collaborators. The operational plan was drafted by the CIA, vetted by the military and approved by the President. For the first time in American history, Special Forces working with CIA operatives were “the lead element in [a] war.” Yet even Secretary of Defense Donald Rumsfeld reportedly questioned who was really in charge. Eleven Special Forces

operations of course being undertaken by the Pentagon pursuant to its war-making authority, Title 50 operations being covert action operations conducted by CIA. Why is that important and fascinating? Because . . . how these cyber-operations are described will dictate how they are reviewed and approved in the executive branch, and how they will be reported to Congress, and how Congress will oversee these activities.” John A. Rizzo, “National Security Law Issues: A CIA Perspective” (University Club, Washington, DC) (May 5, 2010), available at http://www.americanbar.org/content/dam/aba/multimedia/migrated/nationalsecurity/multimedia/ws_30274.mp3 (last visited Mar. 9, 2011).

78 Id.
79 STANTON, supra note 75, at 37. See also GARY SCHROEN, FIRST IN (2005); Henry A. Crumpton, Intelligence and War 2001–2, in JENNIFER E. SIMS, TRANSFORMING U.S. INTELLIGENCE (2005).
80 STANTON, supra note 75, at 33. In past wars, SOF were often the first to enter hostile territory, but they always operated under the command and control of conventional military forces.
81 ROTHSTEIN, supra note 75, at 111. The importance of this point will become apparent later in this paper, but the CIA operatives were working under CIA control and Title 50 authorities while the Special Forces and other military personnel were under the operational control of U.S. Central Command and Title 10 authorities. See BERNTSEN,
teams operated with and coordinated the efforts of indigenous Tajik, Uzbek, Hazar, and Pashtun fighters, who were colloquially referred to as the Northern Alliance. Less than three months later, the Taliban government fell in an archetypal unconventional warfare campaign—small groups of highly skilled personnel operating with indigenous forces against a common enemy.

The U.S. military defines unconventional warfare as "[a]ctivities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area." This definition reveals three defining characteristics of unconventional warfare: 1) it is conducted "by, with, or through" indigenous forces, 2) those indigenous forces are "irregular" (i.e., non-governmental) forces, and 3) it supports "activities" against the government or occupying power.

\[\text{supra note 75, at 86. Notwithstanding their separate lines of authority, the CIA and SOF on the ground in Afghanistan closely coordinated their operations and often operated in concert. In one instance, military commanders initially refused to send a rescue team to the aid of a five-man "CIA" team not realizing that, in fact, three of the five men on the team were active duty military officers. Id. at 287.}\]


\[\text{83 Army Field Manual FM 3-05.130, provides this distinction between regular and irregular forces:}\]

\[\text{Regulars are armed individuals or groups of individuals who are members of a regular armed force, police, or other internal security force . . . Regardless of its appearance or naming convention, if the force operates under governmental control, it is a regular force.}\]

\[\text{Irregulars, or irregular forces, are individuals or groups of individuals who are not members of a regular armed force, police, or other internal security force . . . These forces may include, but are not limited to, specific paramilitary forces, contractors, individuals, businesses, foreign political organizations, resistance or insurgent organizations, expatriates, transnational terrorism adversaries, disillusioned transnational terrorism members, black marketers, and other social or political "undesirables."}\]

\[\text{84 The third characteristic serves to distinguish unconventional warfare from irregular warfare. Irregular warfare is "a violent struggle among state and non-state actors for legitimacy and influence," while unconventional warfare may be waged in support of both conventional state-on-state conflicts and insurgencies.}\]
Activities conducted under the rubric of unconventional warfare include guerilla warfare, subversion, sabotage, intelligence collection, and unconventional assisted recovery. These activities do not necessarily by themselves constitute unconventional warfare, but rather they typify tactics and techniques commonly employed in unconventional warfare. In other words, not all intelligence collection falls under the unconventional warfare umbrella—even when it is conducted by SOF. Nor is guerilla warfare always conducted under the rubric of unconventional warfare.

Unconventional warfare is distinguished from other forms of warfare in that it uses irregular indigenous (surrogate) forces against the established or governing power in denied areas. The indigenous forces may be guerillas waging their own campaign against the government or they may be, essentially, independent agents working for the U.S. government. The indigenous forces have objectives of their own (political or pecuniary), so the mission for U.S. forces is to develop and sustain indigenous capabilities and channel them in ways that simultaneously accomplish U.S. national security objectives. For this reason, unconventional warfare is known colloquially as “by, with, or through.”

The goal of unconventional warfare is to exploit an adversary’s political, military, economic, and psychological vulnerabilities by developing and sustaining indigenous resistance forces to accomplish U.S. objectives. Unconventional warfare is “a classically indirect, and ultimately local, approach to waging warfare.” Unconventional warfare “is fought by subterranean armies composed of volunteers, revolutionists, guerillas, spies, saboteurs, provocateurs, corrupters, [and] subverters,” and it is waged

---

83 ARMY FIELD MANUAL FM 3-05, supra note 83, at 130.
84 “While many of the tactics and techniques utilized within the conduct of UW have significant application and value in other types of special operations, many of these techniques, such as sabotage and intelligence collection, are not exclusive to UW....” LTC MARK GRDOVIC, A LEADER’S HANDBOOK TO UNCONVENTIONAL WARFARE 9 (SWCS Pub 09-1)(2009) (SWCS is an acronym for the U.S. Army John F. Kenneey Special Warfare Center and School located at Ft Bragg, North Carolina).
85 This definition distinguishes unconventional warfare from “foreign internal defense”—a form of surrogate warfare where indigenous regular, or official, forces are trained, equipped, organized, and supported to conduct operations against insurgents or other forms of lawlessness. Prime examples of foreign internal defense are the U.S. military operations to organize, train, and equip government security forces in Iraq and Afghanistan to fight against insurgents. See also id. at 9.
86 ROTHSTEIN, supra note 75, at 159.
through military, political, economic, and psychological means. In peacetime, unconventional warfare "operates at a level below that of outright provocations and the instigators do not appear in the open." A typical general war scenario is when the U.S. military wants to prepare for possible conventional invasion of a foreign country by establishing an unconventional capability (i.e., the ability to use indigenous surrogates). During the preparation phase, which consists of initial contact and infiltration, the goal is to identify exactly what U.S. military needs or requirements would be, as well as which indigenous individuals or groups would be willing to work with U.S. personnel. Initial contact is when contact with resistance forces (potential partners) is first made; this may take place in another country (contacting expatriates or exiles), or through intermediaries such as CIA personnel. Infiltration is when U.S. personnel first enter the country where the potential indigenous partners are located; given the clandestine nature of unconventional warfare, the U.S. personnel will not likely enter the country in uniform, nor will their true intentions be apparent. Organization and buildup are stages where the capabilities of indigenous forces are developed through training and equipping. These indigenous capabilities are then employed to accomplish U.S. objectives. Unconventional warfare concludes with a transition phase that may include

89 Morris Greenspan, *International Law and Its Protection for Participants in Unconventional Warfare*, 341 ANNALS AM. ACAD. POL. & SOC. SCI. 30, 31 (May 1962). Guerilla warfare generally consists of attacks conducted by irregular indigenous forces in areas they do not control. Insurgencies or other armed resistance movements normally use some form of guerilla warfare against the forces they are engaged in conflict with. "Victory is achieved not so much by knocking the enemy's sword from his hand as by paralysing his arm." Charles Townshend, *The Irish Republican Army and the Development of Guerilla Warfare 1916–1921*, 94 ENG. HIST. REV. 318, 318 (1979).

90 Townshend, supra note 89, at 318. Guerilla warfare is typified by "hit-and-run" attacks by forces that do not wear uniforms or openly advertise their armed nature. For example, when Umkhonto, the paramilitary wing of the African National Congress initiated its guerilla campaign against the apartheid government in South Africa in 1961, it "gave first priority to a campaign of sabotage against power and communication facilities and government buildings." Sheridan Johns, *Obstacles to Guerilla Warfare-A South African Case Study*, 11 J. AFR. STUD. 267, 273 (1973).

91 GRDOVIC, supra note 86, at 17.
demilitarization. Historical examples of the U.S. military conducting unconventional warfare in the context of general war include the Jedburgh teams inserted by the Office of Strategic Services (OSS) into occupied France during World War II, Afghanistan in 2001–2002, and Iraq in 2003.

Unconventional warfare in the context of a limited warfare scenario is conducted in very similar phases. The key difference, however, is significant to our purposes here: in limited warfare the U.S. government seeks to apply pressure against an adversary via internal forces rather than a military invasion. In limited warfare, the U.S. government does not use conventional military forces to overtly invade the adversary, but seeks instead to accomplish political objectives through the use of small numbers of SOF, and often CIA personnel, working “by, with, or through” indigenous forces. Limited warfare is politically risky and, thus, conducted in secret: it is colloquially referred to as secret war, dirty war, small war, or low-intensity conflict. The United States conducted unconventional warfare in the context of limited war in North Vietnam in 1961–1964, the


93 ROTHSTEIN, supra note 75, at 27–29. Rothstein also asserts that U.S. forces conducted forms of unconventional warfare in the Revolutionary War, the War of 1812, the Mexican War of 1846–48, the U.S. Civil War and throughout the 20th century.

94 Prior to the initiation of aerial bombardment and the ground campaign in Operation Iraqi Freedom, U.S. Special Forces teams infiltrated northern Iraq and conducted unconventional warfare with Kurdish resistance elements, including the Patriotic Union of Kurdistan. GRODICO, supra note 86, at 7.


96 Unconventional warfare activities in North Vietnam between 1961 and 1964 qualify as being conducted in a limited war context as the U.S. government did not originally intend to introduce conventional military forces in large numbers into Vietnam. It was only after the limited war failed to achieve the desired results that the conflict escalated into general warfare. The Special Observations Group (SOG) was a cover name for a U.S. unconventional warfare task force, composed of SOF. SOG regularly infiltrated North Vietnam and conducted unconventional warfare primarily through intelligence activities, propaganda campaigns, sabotage, and guerrilla attacks. See generally RICHARD H. SHULTZ

Unconventional warfare is generally effectuated in seven phases: preparation, initial contact, infiltration, organization, buildup, employment, and transition.\textsuperscript{98} Each phase may not always be required, and phases may be conducted simultaneously or out of sequence.\textsuperscript{99} Each phase highlights the Title 10-Title 50 debate and related congressional oversight concerns that are the focus of this paper, yet these concerns are particularly acute in the initial contact and infiltration phases. During the initial contact phase, an interagency pilot team “composed of individuals possessing specialized skills” may make contact with indigenous forces and begin assessing the potential to conduct unconventional warfare.\textsuperscript{100} SOF often augment pilot teams led by, and primarily constituted of, CIA personnel.\textsuperscript{101}

\textsuperscript{97} SOF worked with the CIA in supporting various resistance groups in Nicaragua. The operations are generally viewed as an example of how unconventional warfare should not be waged as the resistance groups, collectively referred to as the Contras, never succeeded in building necessary support inside Nicaragua and became viewed as mercenaries with little connection to the local population. See GRDOVIC, supra note 86, at 36.

\textsuperscript{98} ARMY FIELD MANUAL FM 3-05.130, supra note 83, at 4-4.

\textsuperscript{99} “For example, a large and effective resistance movement may require only logistical support, thereby bypassing the organization phase. The phases may also occur out of sequence, with each receiving varying degrees of emphasis. One example of this is when members of an irregular force are exfiltrated to a partner nation (PN) to be trained and organized before infiltrating back into the UWOA [unconventional warfare operating area], either with or without the ARSOF [Army Special Operations Forces] unit. In this case, the typical order of the phases would change.” Id.

\textsuperscript{100} Id. at 4-5. In the context of limited war, the Title 10-Title 50 issues that are the focus of this paper permeate every aspect of the mission. Indeed, the political risks involved and need for secrecy may dictate that the U.S. government not acknowledge its role in the operations, which strikes at the very heart of this debate.

\textsuperscript{101} Id. at 3-2. This manual states it is not unusual for SOF “to augment pilot teams led by and primarily constituted of OGA personnel.” The acronym “OGA” stands for other government agency and is generally understood to be a euphemism for the CIA. See John Henderson, The Conflict In Iraq, L.A. TIMES, Sep. 10, 2004, at A-1. Strictly speaking, a pilot team is not an unconventional warfare mission as much as it is a critical precursor to unconventional warfare. The pilot team’s mission is to conduct a feasibility assessment, which analyzes whether there is an indigenous force with which the U.S. can engage in an unconventional warfare campaign.
This brief overview of unconventional warfare illustrates why unconventional warfare often appears very similar to activities conducted by CIA personnel. Indeed, SOF typically work closely with CIA personnel while conducting unconventional warfare, although the relationship tends to be informal and focused more on mutual support. In other words, the relationship is one of cooperation in pursuit of mutual objectives rather than a formal superior-subordinate relationship. As we will examine in more detail in Part IV of this paper, this is an important distinction that directly answers whether the unconventional warfare mission is a military operation or intelligence activity.

B. Cyberwarfare

Cyberwarfare is no longer the future of warfare—it is the present and future. While a “hot” cyber war between major powers has thankfully not occurred, there are minor skirmishes, a silent cyber arms race, and major intelligence gathering.102 According to Mike Jacobs, formerly of the NSA, countries “are learning as much as they can about power grids and other systems, and they are sometimes leaving behind bits of software that would allow them to launch a future attack.”103 These may be acts of cyber espionage rather than cyberwarfare, but they are at least preparing cyberspace for warfare—and they highlight the integration of intelligence and warfare in cyberspace.

In January 2011, a front-page New York Times article detailed a sophisticated cyberattack straight out of science fiction.104 Strong circumstantial evidence suggested Iran’s nuclear program was delayed for several years after a computer worm named Stuxnet infiltrated the industrial control systems responsible for manufacturing Iran’s nuclear centrifuges. Since the computers controlling Iran’s nuclear enrichment

facilities are not connected to the Internet, Stuxnet was apparently designed to infiltrate the computers of contractors working for Iran’s nuclear program and hitchhike on thumbdrives or similar removable media devices that were later connected to computers at Iran’s enrichment facilities. Stuxnet then caused the machines spinning centrifuges to create defective centrifuges while simultaneously reporting that all systems were performing normally. Experts suggested Stuxnet could only have been created by American or Israeli intelligence agencies. If true, Stuxnet heralded a new age of cyberwarfare able to destroy “targets with utmost determination in military style.”

On June 23, 2009, U.S. Cyber Command was established to lead U.S. military efforts against “cyber threats and vulnerabilities” and “secure freedom of action in cyberspace.” Accepting the recommendation of Secretary of Defense Robert Gates, President Barack Obama nominated Lieutenant General Keith B. Alexander, the Director of the National Security Agency, to also serve as the Commander of U.S. Cyber Command. During the confirmation process, the Senate Armed Services Committee questioned various aspects of General Alexander’s proposed dual responsibilities—questions at the heart of the Title 10-Title 50 debate. How would he carry out his responsibilities as Director of the National Security Agency, an intelligence agency and member of the intelligence community, while also carrying out his responsibilities as Commander of U.S. Cyber Command, a military war-fighting command?

The Committee asked General Alexander, for example, whether the military conducts intelligence gathering of foreign networks, whether intelligence gathering of foreign networks is “authorized and reported to Congress under Title 10 or Title 50,” and whether cyberspace operations are traditional military activities. While many of General Alexander’s answers were provided to the Committee in a classified supplement, his unclassified answers and testimony at his confirmation hearing presumably provide insight into how the Secretary of Defense exercises his statutory and delegated authorities to conduct intelligence activities and military

106 Broad et al., supra note 104.
operations. General Alexander repeatedly explained that “while there will be, by design, significant synergy between NSA and Cyber Command, each organization will have a separate and distinct mission with its own identity, authorities, and oversight mechanisms.”

Cyberspace is defined by the U.S. government as the “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” Others suggest a definition that emphasizes cyberspace as a global information environment unique in its “use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communications technologies.” Indeed, the distinctive use of electronics and electromagnetic spectrum distinguishes cyberspace from the domains of land, sea, air, and space: it is “a physical environment . . . managed by rules set in software and communications protocols.” Cyberspace is governed by the laws of physics and the logic of computer code.

---

108 It is unlikely that General Alexander would have provided written responses to the Committee without such responses being cleared or reviewed by the Secretary of Defense, or at least his subordinates such as the DoD General Counsel. It is also worth noting that while Cyber Command likely possesses significant delegated authorities, the 2011 National Military Strategy specifically calls for “executive and Congressional action to enable effective action in cyberspace.” CHAIRMAN OF THE JOINT CHIEFS OF STAFF, THE NATIONAL MILITARY STRATEGY OF THE UNITED STATES 10 (2011).
109 Hearing on the Nominations of VADM James A. Winnefeld Jr., USN to be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Command; and LTG Keith B. Alexander, USA to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command, S. Comm. on the Armed Services, 105th Cong. 10 (2010).
110 JP 1-02, infra note 115, at 139. This definition is also contained in the 63-day Cyberspace Policy Review directed by President Obama shortly after taking office, which quotes classified NATIONAL SECURITY PRESIDENTIAL DIRECTIVE 54/HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 23 (Jan. 8, 2008).
112 Gregory J. Ratray, An Environmental Approach to Understanding Cyberpower, in CYBERPOWER AND NATIONAL SECURITY, supra note 111, at 254.
113 Id. at 255.
Wikipedia defines Cyberwarfare simplistically: as the use of computers and the Internet to conduct warfare in cyberspace.\textsuperscript{114} The U.S. military does not define cyberwarfare in its unclassified dictionary, wisely avoiding the term "war" with its associated baggage and implications. The U.S. military instead categorizes cyber operations as defense, exploitation, or attack.\textsuperscript{115} This article focuses on the last two categories, exploitation and attack, and attempts to define the legal authorities and identify the type of activities associated with these categories. In the minds of some, exploitation infers intelligence activities while attack sounds like a military operation, yet our analysis here will add nuance to this simplistic characterization.

If the distinguishing characteristics of cyberspace are electronics and electromagnetic spectrum governed by the laws of physics and computer code, then how can we best distinguish cyber exploitation from attack? One could argue that cyber attacks affect electronics and electromagnetic spectrum by altering their physical characteristics or computer code, while exploitation merely gathers information. The problem is that cyber attack thus defined would include acts of computer network exploitation where

\textsuperscript{114} See CYBERWARFARE, WIKIPEDIA http://en.wikipedia.org/wiki/Cyberwarfare [last visited Mar. 7, 2011]. Cyberwar is also defined as referring to "conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems . . . on which an adversary relies to 'know' itself." JOHN ARQUILLA AND DAVID RONFELDT, IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 28 (1997).

\textsuperscript{115} Computer network defense consists of actions "taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks." Computer network exploitation is "[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." Computer network attack consists of actions "taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." All three, defense, exploitation, and attack, fall under the general umbrella term computer network operations U.S. DEPARTMENT OF DEFENSE, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 95 (as amended through Apr. 2010). Examples of cyber operations or activities include mapping networks, scanning networks and industrial control systems (e.g., to find vulnerabilities), denial of service (flooding networks such that they become inoperable), hacking networks or systems to gain stored information (including insertion of malware or spyware), manipulating data on someone else's network or system, taking over control of a system or network so sensors can be turned off or manipulated, activation of malicious code secretly embedded on computer chips during the manufacturing process, and other disruption or destruction of computer networks or systems.
computer code is left behind or altered (for example, keystroke logging or insertion of a "backdoor").

Perhaps cyber attack should be defined or interpreted more in the classical international relations sense of forced political coercion.\footnote{Defining warfare is beyond the scope of this paper, but it suffices to say it involves the forced imposition of political will. It is, in Carl Von Clausewitz's immortal words, the "continuation of political activity by other means." \textsc{Carl Von Clausewitz, On War 87} (Michael Howard & Peter Paret, eds. & trans., Princeton Univ. Press 1976) (1832). \textit{See also Myres S. McDougal & Florentino P. Feliciano, The International Law of War: Transnational Coercion and World Public Order 11} (1994) which defines coercion as "a high degree of constraint exercised by means of any or all of the various instruments of policy."} Cyber operations would not be considered attacks if they seek only to gain information or intelligence, and are not intended to alter or control the primary functions of the adversary's electronics or electromagnetic spectrum—even if they do leave computer code behind, such as keystroke logging software or the insertion of a back door. Subsequent acts to exploit the identified vulnerabilities by asserting control, or coercion, over the systems would rise to the level of attacks.\footnote{Here is a possible definition of cyberwarfare: politically coercive acts that affect electronics and electromagnetic spectrum by altering their physical characteristics or computer code such that the effect is analogous to an armed attack.}

This distinction between merely altering computer code without asserting control or degrading function and actually assuming control or degrading functions is consistent with international law, which does not generally consider intelligence activities to be acts of war. Its weakness, however, is definitional reliance upon the intent of the sponsor. Distinguishing cyber attack from exploitation based on the intent of the sponsor is analogous to the challenge of distinguishing between warning shots and an initiation of armed conflict: intent is clear to the person pulling the trigger, but much less so to those on the receiving end.

The salient point is this: during the initial period after you discover someone is or was inside your network, you may not know whether the other person is initiating an attack or merely attempting to exploit your network. The other party knows why he is inside your network, but you do not. If you know your network is being attacked, a broad range of responses may be justified in self-defense; however, if your network is merely being exploited (an intelligence activity) your range of responses are arguably
more limited. Thus, this distinction helps define the legal authority to carry out an operation, but does little to define appropriate defensive responses.

Which is why intelligence is the key to successful cyberwarfare. Cyber exploitation plays a critical supporting role in cyber attack. Knowing where an adversary’s cyber systems are vulnerable will likely require computer network exploitation “to understand the target, get access to the right attack vantage point, and collect BDA [battle damage assessment].”118 In the words of one expert on cyber attack, “those who prepare and conduct operational cyberwar will have to inject the intelligence operative’s inclinations into the military ethos”—inclinations that include discrete effects, patience, an intuitive understanding of the adversary’s culture, a “healthy wariness of deception, indirection, and concealment . . . [and] a willingness to abandon attack plans to keep intelligence instruments in place.”119

As noted above, the intent or purpose of the actor is typically a key distinction between cyber exploitation and cyber attack. A recent report issued by the National Research Council suggests the distinction is really the nature of the payload, but acknowledges that technical similarities between attack and exploitation “often mean that a targeted party may not be able to distinguish easily between a cyberexploitation and a cyberattack.”120 The Report provides this helpful illustration:

---

118 Martin C. Libicki, Cyberdeterrence and Cyberwar 139 (RAND, 2009).
119 Id. at 156.
This illustration is a helpful starting point, but its simplistic separation of Title 10 and cyber attack in one column and Title 50 and cyber exploitation in another column belies the stovepiped thinking of congressional overseers and ignores current operational realities. It ignores military intelligence collection efforts and operational preparation of the cyber environment by military personnel operating under military command and control—activities that are properly understood to be military operations and not intelligence activities, as we will see in Part IV of this paper.

Cyberwarfare differs from other forms of warfare in that the skills or tools necessary to collect intelligence in cyberspace are often the same skills or tools required to conduct cyber attack. Furthermore, the time lag between collecting information and the need to act upon that information may be compressed to milliseconds. Unlike the traditional warfighting construct where intelligence officers collect and analyze information before passing that information on to military officers who take direct action, cyber attack may require nearly simultaneous collection, analysis, and action. The same government hacker may identify an enemy computer network,
determine its strategic import, and degrade its capabilities all in a matter of seconds.

This is precisely why President Obama put the same man in charge of cyber intelligence activities and military cyber operations. This is also the reason Congress evidenced considerable apprehension and asked many questions about authorities and oversight. After all, congressional oversight retains its antiquated, stovepiped organizational structure and presumes a strict separation between intelligence activities and military operations even when no such separation is legally required.

IV. Distinguishing Military Operations, Intelligence Activities & Covert Action

Title 10 and Title 50 are mutually supporting authorities that can be exercised by the same person or agency, yet congressional oversight is exercised by separate, often competing, committees and subcommittees. This dysfunctional division of congressional oversight of national security is the fundamental “Title 10-Title 50” challenge. Congressional committees exercise oversight and, importantly, authorize and appropriate funds based in part on whether they perceive an activity to be an intelligence activity or a military operation.

The question of whether an unconventional or cyber warfare activity is a military operation, an intelligence activity, or covert action is more precisely a question of congressional oversight: will the intelligence committees exercise primary oversight jurisdiction, or will the armed services committees? To answer this question, we will first define intelligence activities and identify the key elements that distinguish military operations from intelligence activities. We will then examine covert action, which is not synonymous with intelligence activities despite that persistent misperception, and we will learn why even unacknowledged military operations may be exempt from intelligence committee oversight. Our analysis of the relevant statutes will reveal that traditional military activities are not intelligence activities or covert action. A brief review of military and legislative history will show that military operations preparatory to anticipated conflict are traditional military activities, and that even unacknowledged operations by military personnel under military command and control may not constitute covert action.
A. Military Operation or Intelligence Activity?

Title 50 directs the President “to ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States,” yet there is no statutory definition of the term “intelligence activities.” The closest Title 50 comes to defining intelligence activities is its stipulation that the term includes “covert action” and “financial intelligence activities.” Other provisions in Title 50 appear to suggest that “military intelligence activities” and “tactical intelligence activities” are distinguishable from (rather than subsets of) intelligence activities. This distinction is supported by the statutory definition of the National Intelligence Program, which provides that it “does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.”

Executive Order 12,333 broadly defines intelligence activities as “all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.” The Intelligence Community includes elements from several government agencies, including the CIA, the Department of State, the Department of Treasury, the Department of Energy, and, naturally, DoD. Indeed, so many elements of DoD are also

---

122 Id. § 413(a)(1), (f) (2006).
123 See 50 U.S.C. § 403-3(a) (2006), which expresses the sense of Congress that either the DNI or his Deputy should have experience with or appreciation of “military intelligence activities,” and 50 U.S.C. § 403-5(a)(3) (2006), which directs the Secretary of Defense to coordinate with the DNI to “ensure that the tactical intelligence activities of [DoD] complement and are compatible with intelligence activities under the National Intelligence Program.”
125 E.O. 12,333, supra note 10, § 3.5(g).
126 Both Title 50 U.S.C. § 401a(4) (2006) and Executive Order 12,333 define the Intelligence Community as including:

(A) The Office of the Director of National Intelligence.
(B) The Central Intelligence Agency.
(C) The National Security Agency.
(D) The Defense Intelligence Agency.
(E) The National Geospatial-Intelligence Agency.
(F) The National Reconnaissance Office.
members of the Intelligence Community—and E.O. 12,333 gives those elements broad authority to carry out intelligence activities—that the statutory distinction between intelligence activities and military intelligence activities we saw in the preceding paragraph is nearly obviated.  

This jumble of defined and undefined terms leads to the confusion discussed throughout this Article about where to draw the line between intelligence activities and military operations. Yet the critical distinction emerges when E.O. 12,333 Sec. 1.10 assigns distinct responsibilities to the Secretary of Defense to: "(a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director; (b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's

---

(G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.
(H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy.
(I) The Bureau of Intelligence and Research of the Department of State.
(J) The Office of Intelligence and Analysis of the Department of the Treasury.
(K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard.
(L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

Title 50 U.S.C. § 401a(4) (2006). See also E.O. 12,333 supra note 10, § 3.5(h) (defining the elements of the Intelligence Community).

127 For example, the intelligence and counterintelligence elements of the Army, Air Force, Navy, and Marine Corps are part of the Intelligence Community, and E.O. 12,333 directs those elements to "[c]ollect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements . . . ." E.O. 12,333, supra note 10, at § 1.7(f)(1). Thus, E.O. 12,333 authorizes elements of DoD to conduct military ("departmental") intelligence activities and national intelligence activities.
responsible.\textsuperscript{128} The primary question, then, is whether the activity is being conducted in response to tasking from the DNI or the Secretary of Defense.

The foregoing suggests a two-part test to determine whether an activity is an intelligence activity or a military operation. An intelligence activity is: (1) conducted by an element of the intelligence community (2) in response to tasking from the DNI. If the activity in question fulfills both requirements, then it is an intelligence activity authorized primarily by Title 50. If the activity is conducted by a DoD element of the intelligence community pursuant to tasking from the Secretary of Defense, then it should be considered a military operation, or military intelligence activity, conducted under either Title 10 or Title 50 authority.\textsuperscript{129} If the activity is conducted by a DoD element that is not part of the Intelligence Community, then the activity is a military operation conducted only under Title 10 authority.

This discussion highlights why the Title 10-Title 50 debate is typically little more than a debate about congressional oversight. The Secretary of Defense possesses authorities under both Title 10 and Title 50. The armed services committees exercise oversight over all DoD activities and operations, including military intelligence activities, tactical intelligence activities, and other departmental intelligence-related activities. The

\textsuperscript{128} EO 12,333, \textit{supra} note 10, at § 1.10. This distinction is reinforced in subsection (c) where the Secretary of Defense is given authority to "conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements."

\textsuperscript{129} The Secretary of Defense may direct DoD personnel to carry out intelligence activities in response to national intelligence requirements, or to meet the intelligence needs of the military. When DoD personnel conduct intelligence activities in response to national intelligence requirements, they do so primarily under Title 50 authorities (50 U.S.C. § 403-5(b)(1) (2006)) and pursuant to priorities and needs determined by the DNI (50 U.S.C. § 403-1(f) (2006)). When DoD personnel conduct intelligence activities to fulfill military intelligence requirements, those intelligence activities are conducted under Title 10 authorities, e.g., 10 U.S.C. §§ 113, 164 (2006), and delegated authorities from the President and Secretary of Defense; if the DoD personnel are also members of the Intelligence Community (e.g., NSA) the activities are also conducted pursuant to Title 50 authorities (50 U.S.C. § 403-5 (2006). These military operations are also sometimes referred to as "DoD Intelligence Related Activities" or "Tactical Intelligence and Related Activities (TIARA)."

challenge is that the intelligence committees also want to assert jurisdiction over the "intelligence-related" activities of the military.

As we saw in Part II, the intelligence committees purport to exercise broad jurisdiction over all intelligence-related activities, including those of the military, which in turn creates overlapping jurisdiction with the armed services committees and needlessly generates confusion over oversight and reporting requirements. While the intelligence committees may be justified in asserting jurisdiction over DoD activities authorized and funded under Title 50 authorities, the same cannot be said of DoD intelligence-related activities authorized and funded under Title 10 authorities. These Title 10 activities should be properly categorized as military operations subject to the exclusive oversight of the armed services committees.

B. Is the Military Operation a Covert Action?

The military operations discussed in Part III, unconventional and cyber warfare, are conducted by SOF and U.S. Cyber Command, respectively. Neither special operations nor U.S. Cyber Command are elements of the Intelligence Community, so if an unconventional or cyber warfare activity is conducted pursuant to tasking from the Secretary of Defense, then there can be little question it is a military operation. Military operations authorized and funded under Title 10 authorities are properly labeled military operations subject to the exclusive oversight of the armed services committees, even if those activities are related to intelligence gathering — so long as they are in response to tasking from the Secretary of Defense and remain under military direction and control. Yet Title 50 includes one provision that would place even military operations meeting these criteria under the jurisdiction of the intelligence committees: the intelligence committees retain jurisdiction over all covert action.

For all that is lacking in the Title 50 definition of intelligence activities, it does stipulate that the term includes "covert action." Indeed, covert action is arguably the intelligence activity that generates the most attention and concern, especially from members of Congress. The very phrase conjures images of cloak-and-dagger intrigue and rogue actors manipulating foreign powers while possessing "a license to kill." For most of American history, the term covert action was not statutorily defined — and had little reason to be — until Congress became concerned with oversight.

\[^{130}\text{50 U.S.C. § 413(a)(1), (f) (2006).}\]
Indeed, President George H.W. Bush issued a signing statement calling Congress's definition of covert action "unnecessary" and stated he would continue to consider the historic missions of the U.S. military in determining whether a particular activity constituted a covert action.\footnote{131}

Following the Iran-Contra affair, Congress statutorily defined covert action as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."\footnote{132} Accordingly, covert action consists of three essential elements:

\footnote{131} President Bush's signing statement reads, in pertinent part:

\begin{quote}
I believe that the Act's definition of "covert action" is unnecessary. In determining whether particular military activities constitute covert actions, I shall continue to bear in mind the historic missions of the Armed Forces to protect the United States and its interests, influence foreign capabilities and intentions, and conduct activities preparatory to the execution of operations.
\end{quote}

Statement on Signing the Intelligence Authorization Act, Fiscal Year 1991, in BOOK II PUB. PAPERS 1043–44 (1991). The use of Presidential signing statements is controversial. Some scholars view signing statements as an attempt to influence legislative history by creating "executive...history that is expected to be given weight by the courts in ascertaining the meaning of statutory language." Marc N. Garber & Kurt A. Wimmer, Presidential Signing Statements as Interpretations of Legislative Intent: An Executive Agrandizement of Power, 24 HARV. J. ON LEGIS. 363, 366 (1987). Nevertheless, the Constitution does envision a significant Presidential role in the legislative process, see, e.g., U.S. CONST. art. I, § 7, cl. 2, and some courts have relied on signing statements when interpreting legislation. See, e.g., United States v. Story, 891 F.2d 988, 994 (2d Cir. 1989); Berry v. Dep't of Justice, 733 F.2d 1343, 1349–50 (9th Cir. 1984); Clifton D. Mayhew, Inc. v. Wirtz, 413 F.2d 658, 661–62 (4th Cir. 1969). However, signing statements are probably entitled to no more consideration than other forms of "post-passage legislative history, such as later floor statements, testimony or affidavits by legislators, or amicus brief filed by members of Congress." Walter Dellinger, Memorandum for Bernard M. Nussbaum, Counsel to the President, The Legal Significance of Presidential Signing Statements (Nov. 3, 1993), 17 Op. O.L.C. 131, 134 (1993).

\footnote{132} 50 U.S.C. § 413b(c) (2006). A year after its creation by the National Security Act of 1947, the National Security Council issued NSC Directive 1012, which established a policy of containment of the Soviet Union and redefined covert action. Originally drafted by George Kennan, then director of the State Department's Policy Planning Staff, "NSC 1012 was the turning point for covert action, expanding it from propaganda to direct intervention." NSC Directive 1012 defined covert action to include "propaganda, economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to
1. An activity of the U.S. government;
2. To influence political, economic, or military conditions abroad; and
3. Where it is intended that the role of the U.S. government will not be apparent or acknowledged openly.

This definition was included in the Intelligence Authorization Act for 1991. The accompanying Conference Report emphasized that Congress did not intend for the definition to expand or contract previous definitions of covert action; rather, the intent was to "clarify the understandings of intelligence activities that require presidential approval and reporting to Congress." The Senate Report, which was not adopted in whole by the Conference Report, stressed that "the core definition of covert action should be interpreted broadly." It is not clear that the Executive Branch shares Congress's interpretation, nor are these congressional interpretations legally binding. Nevertheless, the first element, "an activity of the U.S. government," naturally includes any activity by U.S. government personnel, as well as any activity by third parties acting on behalf of U.S. government underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anticomunist elements." The Directive stipulated that covert action was to be "so planned and executed that any U.S. Government responsibility for them is not evident to unauthorized persons and that if uncovered the U.S. Government can plausibly disclaim any responsibility for them." This definition guided U.S. government actions for over forty years. Teverton, supra note 10, at 210.

136 Statements in committee reports may provide persuasive authority, but do not have the force of law. American Hospital Assn. v. NLRB, 499 U.S. 606, 616 (1991); TVA v. Hill, 437 U.S. 153, 191 (1978) ("Expressions of committees dealing with requests for appropriations cannot be equated with statutes enacted by Congress.").
personnel and under their control. The second element— influencing political, military or economic conditions abroad— was intended by Congress (or at least the Senate intelligence committee) to include nearly all “activities to influence conditions” abroad; this purports to be an objective test, and it was not intended to require an articulable link to specific foreign policy or defense objectives. The third and “essential element of a covert action is that the role of the United States in the activity is not apparent and not intended to be acknowledged at the time it is undertaken.” The Conference Report stressed an activity is not covert action “unless the fact of United States government involvement in the activity is itself not intended to be acknowledged.”

Importantly, “covert action” is a noun, which suggests that covert may be used as an adverb in situations that do not amount to covert action. Additionally, the statutory definition of covert action makes no distinction between kinetic activities (e.g., direct action like the operation to kill or capture Osama bin Laden) or nonkinetic activities (e.g., intelligence gathering). What turns a covert activity into “covert action” is its intended effect— influencing conditions abroad.

Returning to our analysis here, any U.S. military operation abroad would certainly meet the first and second element. The first element would be objectively met if the military operation was conducted by U.S. military personnel. Unconventional warfare could potentially require further analysis, but the existence of an unconventional warfare execute order would certainly suggest the pertinent third parties would be under some

---

137 50 U.S.C. § 413b(e) (2006). Under the control of U.S. government personnel includes “receiving direction and assistance . . . significant financial support or other significant forms of tangible material support . . . .”
138 At the time of this legislation, the working definition of “special activities” (a euphemism for covert action) in E.O. 12,333 included this element: “in support of national foreign policy objectives abroad.” The Senate Report rejected this element as written because it wanted to eliminate the arguable distinction between foreign policy and defense policy, which had been invoked by the executive branch. Id.
140 H.R. REP. NO. 102-166, supra note 129, at 29. The Report acknowledges that “it is not possible to craft a definition of ‘covert action’ so precise as to leave no areas of ambiguity in its potential application.”
141 JOINT PUBLICATION 5-0, JOINT OPERATION PLANNING (Dec. 26, 2006) at GL-9, GL-11 and I-25 [hereinafter JP 5-0]. An Execute Order is an “order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to implement a decision by the President to initiate military operations.” Id. at GL-9.
form of U.S. control. The second element would similarly be easily established, as it is difficult to imagine a military operation abroad that would not have some objective influence on conditions abroad (accepting the Senate intelligence committee’s view that the qualifiers “political, military, or economic” are intended to be all-encompassing). Indeed, it is difficult to understand why a military operation would be conducted abroad but for intent to influence conditions. The third “essential” element, then, is key: a military operation could be deemed covert action if it is not intended to be acknowledged.

Simple statutory interpretation suggests several points relevant to our analysis of the acknowledgement element. The first point is simply that acknowledgement must be “intended” at the time the operation is initiated. Circumstances change, but if the U.S. government intends to acknowledge its involvement at the time the military operation is planned and executed, then it is not covert action. The requirement of intention also removes any requirement of actual acknowledgement; whether the operation is actually acknowledged is immaterial, so long as acknowledgement was intended at the time the operation commenced. Second, operational security is distinguishable from attribution—concealment or misrepresentation do not imply or suggest lack of acknowledgement. Military personnel may take great pains to conceal their true identity, but that does not make an operation covert if the intent remains to acknowledge U.S. government involvement at some unspecified time. Third, the statute does not state when the operation must be acknowledged. The legislative history is silent on this point as well, which leaves considerable room for reasonable interpretation by the executive branch. Conceivably, an intention to acknowledge U.S. government involvement two years after the conclusion of the military operation still negates the “is not intended to be acknowledged” element. Fourth, Webster’s Dictionary defines “acknowledge” as “to admit to be real or true,” which implies it is in response to a query or question.¹⁴² The U.S. government need not promulgate a press release or make a formal announcement of its involvement in the military operation. Indeed, if the operation is conducted without detection, or if the U.S. government is never asked whether it was

¹⁴² Webster’s further explains: “ACKNOWLEDGE implies making a statement reluctantly, often about something previously denied.” WEBSTER’S UNABRIDGED DICTIONARY 17 (Random House, 2d ed. 2001). In the absence of a statutory definition, the courts will generally “construe a statutory term in accordance with its ordinary or natural meaning.” FDIC v. Meyer, 510 U.S. 471, 476 (1994).
responsible for the operation, then the need to acknowledge would not be triggered. The courts generally interpret statutes in a way that gives effect to every word,\footnote{Bailey v. United States, 516 U.S. 137, 146 (1995) ("[W]e assume that Congress used two terms because it intended each term to have a particular, nonsuperfluous meaning"); Montclair v. Ramsdell, 107 U.S. 147, 152 (1883).} which means the intent and acknowledgment elements should be considered independently. In other words, there may be intent to acknowledge without actual acknowledgement, just as there may not be an intent to not acknowledge (deny) that is not exercised because the operation is never discovered.

If a military operation fails any of the three requisite elements in the definition of covert action, it is not covert action. However, even if a military operation meets all three elements, the military operation may still not be covert action. After defining covert action, the statute next lists several exclusions. Covert action "does not include":

(1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
(2) traditional diplomatic or military activities or routine support to such activities;
(3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
(4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.\footnote{50 U.S.C. § 413b(e)(1)-(4) (2006) (emphasis added). The Conference Report that accompanied this statutory definition stated these exclusions "do not fall within the definition of covert action":}

\begin{enumerate}
\item activities where the primary purpose is to collect intelligence;
\item traditional counterintelligence activities;
\item traditional operational security programs and activities;
\item administrative activities (e.g., pay and employee support);
\item traditional diplomatic activities and their routine support;
\item traditional military activities and their routine support;
\item traditional law enforcement activities and their routine support; or
\item routine support to the overt activities of the U.S. government.
\end{enumerate}
Thus, even unacknowledged unconventional or cyber warfare activities are not covert action if they are a "traditional military activity" or if they could be considered "routine support" to a traditional military activity.

1. Traditional Military Activities are not Covert Action

While several of the activities excluded from the definition of covert action could apply to unconventional and cyber warfare depending on the context and actors involved, our analysis will focus on traditional military activities because of their greater relevance and implications for congressional oversight. The accompanying Conference Report explicitly excludes "traditional military activities" and "routine support" from the definition of covert action, before providing this crucial insight into what Congress intended:

It is the intent of the conferees that "traditional military activities" include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and for operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly. In this regard, the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander. Activities that are not under the direction and

145 If the primary purpose of an activity is to collect intelligence, then presumably such activities would be considered "intelligence activities" under E.O. 12,333, and the intelligence committees would exercise oversight. However, defining an activity as a traditional military activity places the activity under oversight of the armed services committees. The congressional intelligence committees fear that the military prefers the less intrusive oversight of the armed services committees and, thus, incorrectly defines all military intelligence-related activities as traditional military activities.
control of a military commander should not be considered as "traditional military activities."\textsuperscript{146}

The Conference Report test for traditional military activities suggests four elements. Traditional military activities are:

1. conducted by U.S. military personnel,
2. under the direction and control of a U.S. military commander,
3. preceding and related to anticipated hostilities or related to ongoing hostilities involving U.S. military forces, and
4. the U.S. role "in the overall operation is apparent or to be acknowledged publicly"

Elements 1 and 2 are relatively straightforward: traditional military activities must be conducted, directed, and controlled by U.S. military personnel. Element 2, military command and control, distinguishes traditional military activities from any situation in which special operations personnel are seconded to the CIA and operating under the direction and control of CIA personnel.\textsuperscript{147} The most recent example of such a scenario was the operation to kill or capture Osama bin Laden, which is discussed in the introduction to this Article. The chain of command, as described by Panetta, apparently ran from the President to the Director of Central Intelligence to the Commander of Joint Special Operations Command.\textsuperscript{148} As the operation was conducted under the direction and control of the CIA and was not (originally) intended to be acknowledged, the operation could not be considered a traditional military activity and was classified as covert action.

Element 2, or direction and control, will not necessarily be dispositive because the Secretary of Defense is authorized by law and executive order to conduct intelligence activities and military operations. As we saw in Part II, the Secretary of Defense's statutory authorities are grounded in his Title 10 authorities as head of DoD (e.g., 10 U.S.C. §113), his Title 10 intelligence authorities (e.g., 10 U.S.C. § 137), his Title 50

\textsuperscript{146} Conference Report, supra note 129 (emphasis added).

\textsuperscript{147} In 1962, President John F. Kennedy issued National Security Action Memorandum 162, which assigned Army Special Forces ("Green Berets") to support CIA covert paramilitary operations and even directed DoD to provide funding to those CIA-led operations. ROTHSTEIN, supra note 75, at 38.

\textsuperscript{148} See supra note 2 and accompanying text.
intelligence authorities (e.g., 50 U.S.C. §403-5), and his delegated authorities contained in Executive Order 12,333 and elsewhere.\footnote{The Secretary of Defense may direct DoD personnel to carry out intelligence activities in response to national intelligence requirements, or to meet the intelligence needs of the military. When DoD personnel conduct intelligence activities in response to national intelligence requirements, they do so primarily under Title 50 authorities (50 U.S.C. § 403-5(b)(1) (2006)) and pursuant to priorities and needs determined by the Director of National Intelligence (50 U.S.C. § 403-1(f) (2006)). When DoD personnel conduct intelligence activities to fulfill military intelligence requirements, those intelligence activities are conducted under Title 10 authorities, e.g., 10 U.S.C. §§ 113, 164 (2006), and delegated authorities from the President and Secretary of Defense; if the DoD personnel are also members of the Intelligence Community (e.g., the National Security Agency) the activities are also conducted pursuant to Title 50 authorities (50 U.S.C. § 403-5 (2006)).}

Element 3 introduces the subjective terms ‘preceding and related to’ and ‘anticipated’ hostilities. These terms raise several questions: how far in advance does ‘preceding’ include, how closely ‘related’ must the activities and hostilities be, and does ‘anticipated’ imply imminence or require a high probability of occurrence? With respect to the word ‘anticipated,’ the Conference Report provides some clarity by stating that ‘anticipated’ means ‘approval has been given by the National Command Authorities for the activities and for the operational planning for hostilities.’\footnote{Conference Report, supra note 129, at 30. The ‘National Command Authorities’ are the President and Secretary of Defense. JP 5-0, JOINT OPERATION PLANNING (Dec. 26, 2006) at GL-9.} Such approval is evidenced by the existence of a Planning Order, Warning Order, or Execute Order issued at the direction of the Secretary of Defense.\footnote{JP 5-0, supra note 141, at GL-11 and I-25. The issuance of an Execute Order is no mere technicality. Execute Orders are typically preceded by Planning Orders and a planning phase, so the Execute Order signals the transition from planning to operations. A Planning Order is a ‘directive that provides essential planning guidance and directs the initiation of execution planning before the directng authority approves a military course of action.’ Id. at GL-20.} Thus, actual hostilities will be obvious and anticipated hostilities will be evidenced by an order of some sort, so any ambiguity with respect to element 3 will likely center on the phrase ‘preceding and related to.’

Congress did not define ‘preceding and related to,’ but the Conference Report stressed that ‘the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander.’\footnote{Conference Report, supra note 129, at 30.} This point is particularly illuminating as the
Conference Report next suggests that unacknowledged “activities undertaken well in advance of a possible or eventual U.S. military operation” will be deemed covert action unless they can be considered “routine support” to the anticipated military operation.\textsuperscript{153}

“Routine support” as defined by Congress includes “cacheing communications equipment or weapons, the lease or purchase from unwitting sources of residential or commercial property to support an aspect of an operation, or obtaining currency or documentation for possible operational uses, if the operation as a whole is to be publicly acknowledged.”\textsuperscript{154} The report continues:

The Committee would regard as "other-than-routine" support activities undertaken in another country that involve other than unilateral activities. Examples of such activity include clandestine attempts to recruit or train foreign nationals with access to the target country to support U.S. forces in the event of a military operation; clandestine effects to influence foreign nationals of the target country concerned to take certain actions in the event of a U.S. military

\textsuperscript{153} \textit{Id.} The Conference Report then refers readers to the Senate Report, which states

\textsuperscript{154} Conference Report, \textit{supra} note 129, at 30.
operation; clandestine efforts to influence and effect public opinion in the country concerned where U.S. sponsorship of such efforts is concealed; and clandestine efforts to influence foreign officials in third countries to take certain actions without the knowledge or approval of their government in the event of a U.S. military operation.\textsuperscript{155}

The Conference Report defines traditional military activities and stresses that military "direction and control" is a deciding factor. The Conference Report then defers to the Senate Report to further define "routine support" of traditional military activities, which then introduces the distinction between unilateral activities and the use of foreign nationals. Read in context, the "routine support" definition only applies to activities that are not under the direction and control of a military commander.\textsuperscript{156}

To summarize, an essential element of covert action is lack of intended acknowledgement of the overall operation, so the existence of intended acknowledgement obviates any need for further analysis under the traditional military activities exception. The only time the military would need to concern itself with analysis under the traditional military activities exception is when the specific military operation is not intended to be acknowledged. In that situation, the next analytical step is to determine whether the specific unacknowledged military operation is a traditional military activity. If an unacknowledged activity is 1) conducted by military personnel, 2) under military direction and control, and 3) pursuant to an order issued or authorized by the Secretary of Defense, then the only remaining requirement to escape falling within the definition of covert action is that 4) the U.S. role in the overall anticipated military operation must be acknowledged. Notwithstanding this relatively straightforward analysis, military preparatory operations continue to raise congressional ire.

\textsuperscript{155} Id.

\textsuperscript{156} It is inconceivable that U.S. military personnel would conduct an activity overseas without the existence of an authorization order from the Secretary of Defense. Thus, the routine support provision seems intended to address those situations where non-military personnel are used to provide support to anticipated military operations. Read as such, Congress's distinction between unilateral activities and those involving foreign nationals seems logical.
2. Military Preparatory Operations are Traditional Military Activities

Over the past ten years, members of the congressional intelligence committees repeatedly expressed frustration with what they see as DoD's deliberate side-stepping of their oversight by renaming intelligence activities as "operational preparation of the environment."157 These congressional concerns are most commonly raised in the context of intelligence activities conducted during the period preceding hostilities. This is the period where conflict is portended but not yet inevitable: when military forces begin making preparations for possible conflict. These preparatory operations are what the U.S. military calls "operational preparation of the environment," or OPE.

In its report accompanying the Intelligence Authorization Act for 2010, HPSCI criticized DoD for frequently labeling its clandestine activities as OPE "to distinguish particular operations as traditional military activities and not as intelligence functions" and, implicitly, escape intelligence oversight.158 HPSCI opined that this practice made the distinction all but meaningless as DoD "has shown a propensity to apply the OPE label where the slightest nexus of a theoretical, distant military operation might one day exist."159 HPSCI argues that this practice obfuscates the military operations from congressional oversight, yet our analysis in Part II revealed that oversight of OPE should still be exercised by the armed services committee.160

A fundamental concern of the intelligence committees is that DoD's clandestine activities labeled as OPE "carry the same diplomatic and

158 House Permanent Select Committee on Intelligence, Report Accompanying the Intelligence Authorization Act for Fiscal Year 2010, 111th Congress, 2nd Session, at 10 (Jun. 25, 2009). This bill was passed by the House but not by the Senate. In fact, the House and Senate have failed to enact an intelligence authorization act for the past five years. The Intelligence Community is able to spend appropriations only because of the unique provision of 10 U.S.C. § 413 (2006), which pre-authorizes intelligence appropriations.
159 Id. at 11.
160 See, e.g., the written questions posed to General Keith Alexander by the Senate Armed Services Committee prior to his confirmation as Commander of U.S. Cyber Command.
national security risks as traditional intelligence-gathering activities.”\textsuperscript{161} Where Title 50 requires that the intelligence committees be kept “fully and currently informed” of all intelligence activities, Title 10 does not have a corresponding requirement that the armed services committees be kept informed of all military operations. More importantly, the intelligence committees fear that DoD is skirting the formal Presidential approval and reporting requirements for covert action by evasively naming equivalent activities as OPE.\textsuperscript{162}

Clandestine activities are generally distinguished from covert activities in that clandestine activities are conducted secretly, but if activity is discovered the role of the United States will ultimately be acknowledged.\textsuperscript{163} If the U.S. government intends to acknowledge the clandestine activities at some point, then they fail the third definitional element for covert action. If the U.S. government does not intend to acknowledge clandestine activities of the U.S. military, then the question becomes whether those clandestine activities are traditional military activities. If so, then the statutory covert action paradigm does not apply as a matter of law.

The Senate Select Committee on Intelligence expressed frustration in 2009 with what it viewed as overly broad interpretations of traditional military activities by the Executive Branch. In questions submitted to Admiral Dennis Blair, the nominee for Director of National Intelligence, and Leon Panetta, then the nominee for the position of Director of Central Intelligence, SSCI asked both nominees to distinguish “between covert action, military support operations, and operational preparation of the

\textsuperscript{161} HPSIC Report, supra note 158, at 11.

\textsuperscript{162} See Nomination of General Michael V. Hayden USAF to be Director of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence, 109th Cong., 2d Sess. 26–7 (May 18, 2006).


An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities.”

JP 1-02, supra note 115, at 89.
environment.”\textsuperscript{164} Blair responded that there is “often not a bright line between these operations” and, thus, they “must be very carefully considered and approved by appropriate authorities and they must be coordinated thoroughly in the field.”\textsuperscript{165}

Panetta answered by correctly emphasizing that covert action is defined by statute to be actions “where the role of the U.S. will not be acknowledged” and “[t]raditional military activities are exempt from the definition.”\textsuperscript{166} Panetta opined that “the line between covert actions under Title 50 and clandestine military operations under Title 10 has blurred” and expressed concern that “Title 10 operations, though practically identical to Title 50 operations, may not be subjected to the same oversight as covert actions, which must be briefed to the Intelligence Committees.”\textsuperscript{167}

When Panetta stated “the line between covert actions under Title 50 and clandestine military operations under Title 10 has blurred,” he seems to have meant that the activities in question appear increasingly similar—not that the statutory authorities to conduct the activities have blurred. General Michael Hayden emphasized this distinction during his confirmation hearings prior to becoming Director of the NSA: OPE and foreign intelligence gathering may appear similar in terms of “tradecraft” but the “legal blood line[s]” are different—“different authorities, somewhat different purposes, mostly indistinguishable activities.”\textsuperscript{168}

\textsuperscript{164} Here is the Committee’s complete question: “As you know, the Under Secretary of Defense for Intelligence has Title 10 and Title 50 authorities. The USDI was dual-hatted by DNI McConnell to serve concurrently as his Deputy Director for Defense. Yet, the USDI has, on occasion, asserted that this Committee does not have primary jurisdiction over his programs. This is of particular concern to this Committee as the USDI has interpreted Title 10 to expand “military source operations” authority, allowing the Services and Combatant Commands to conduct clandestine HUMINT operations worldwide. These activities can come awfully close to activities that constitute covert action.” Nomination of the Honorable Leon E. Panetta to be Director, Central Intelligence Agency: Hearing Before S. Select Comm. on Intelligence, 111th Cong., 1st Sess. 94 (2009); Nomination of Dennis C. Blair to be Director of National Intelligence: Hearing Before the S. Select Comm. on Intelligence, 111th Cong., 1st Sess. 116 (2009).

\textsuperscript{165} Blair, supra note 164, at 117.

\textsuperscript{166} Questions for the Record, Nomination of the Honorable Leon E. Panetta to be Director, Central Intelligence Agency: Hearing Before S. Select Comm. on Intelligence, 111th Cong., 1st Sess. 94 (2009), available at http://intelligence.senate.gov/090205/panetta_post.pdf.

\textsuperscript{167} Id.

\textsuperscript{168} Nomination of General Michael V. Hayden USAF to be Director of the Central Intelligence Agency, Hearing Before the S. Select Comm. on Intelligence, 109th Cong., 2d Sess. 116 (May 18, 2006). General Hayden continued,
The concern of the intelligence committees, then, is that the military is increasingly conducting activities that appear very similar to activities conducted by the CIA and other members of the intelligence community, yet those activities are not subject to the oversight of the intelligence committees. These secret military activities are not covert action because they are either intended to be acknowledged at some point or they are traditional military activities. The intended acknowledgement element is difficult to argue against, so the intelligence committees seem to be centering their arguments for oversight of the military’s secret activities by suggesting that these are not actually traditional military activities.

Unacknowledged unconventional or cyber warfare may legally be conducted when directed by the President and Secretary of Defense in preparation for an anticipated conventional conflict, and those unacknowledged activities are excluded from the definition of covert action. Put another way, if the unconventional or cyber warfare activity at issue can be considered a “traditional military activity,” then it is not covert action; if the activity at issue is “routine support” to a traditional military activity,” then it is not covert action. Neither exclusion from the definition of covert action makes any reference to whether the activity at issue will be acknowledged by the U.S. government should its existence become public.

VI. Conclusion

This article identified four general concerns that are colloquially described as “Title 10-Title 50” issues. Two concerns, military transparency and rice bowls, fall squarely within the policy realm. They are genuine

My view is that, as the national HUMINT manager, the Director of CIA should strap on the responsibility to make sure that this thing down here that walks and quacks and talks like human intelligence is conducted to the same standards as human intelligence without questioning the Secretary’s authority to do it or the legal authority under which that authority is drawn.

*Id.*

concerns, but generally reflect policy concerns, including a competition for scarce resources, rather than legal challenges. Military leaders must vigilantly ensure the U.S. military retains the respect and admiration of the American public and executive branch bureaucrats will always seek to protect their domains, but debates over transparency and rice bowls should not keep military operators awake at night. On the other hand, the critical questions of operational authorities and congressional oversight are central to our national security framework and must be carefully defined and understood by operators and policy-makers alike.

Congress's failure to provide necessary interagency authorities and budget authorizations threatens our ability to prevent and wage warfare. Congress's stubborn insistence that military and intelligence activities inhabit separate worlds casts a pall of illegitimacy over interagency support, as well as unconventional and cyber warfare. The U.S. military and intelligence agencies work together more closely than perhaps at any time in American history, yet Congressional oversight and statutory authorities sadly remain mired in an obsolete paradigm. After ten years of war, Congress still has not adopted critical recommendations made by the 9/11 Commission regarding congressional oversight of intelligence activities. Congress's stovepiped oversight sows confusion over statutory authorities and causes Executive Branch attorneys to waste countless hours distinguishing distinct lines of authority and funding. Our military and intelligence operatives work tirelessly to coordinate, synchronize, and integrate their efforts; they deserve interagency authorities and Congressional oversight that encourages and supports such integration.
SYNOPSIS OF THE UNITED STATES

CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE, ET AL. v. AMNESTY INTERNATIONAL USA ET AL.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT


Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U. S. C. § 1881a, added by the FISA Amendments Act of 2008, permits the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not “United States persons” and are reasonably believed to be located outside the United States. Before doing so, the Attorney General and the Director of National Intelligence normally must obtain the Foreign Intelligence Surveillance Court’s (FISC) approval. Surveillance under § 1881a is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment. Respondents—attorneys and human rights, labor, legal, and media organizations—are United States persons who claim that they engage in sensitive international communications with individuals who they believe are likely targets of § 1881a surveillance. On the day that the FISA Amendments Act was enacted, they filed suit, seeking a declaration that § 1881a is facially unconstitutional and a permanent injunction against § 1881a–authorized surveillance. The District Court found that respondents lacked standing, but the Second Circuit reversed, holding that respondents showed (1) an “objectively reasonable likelihood” that their communications will be intercepted at some time in the future, and (2) that they are suffering present injuries resulting from costly and burdensome measures they take to protect the confidentiality of their international communications from possible § 1881a surveillance.

Held: Respondents do not have Article III standing. Pp. 8–24.

(a) To establish Article III standing, an injury must be “concrete,
Syllabus

particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.

Monocento Co. v. Geertson Seed Farms, 561 U.S. 151 (2010). "[T]hreatened injury must be "certainly impending" to constitute injury in fact, and "[a]llegations of possible future injury" are not sufficient.


(b) Respondents assert that they have suffered injury in fact that is fairly traceable to §1881a because there is an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted under §1881a at some point. This argument fails. Initially, the Second Circuit's "objectively reasonable likelihood" standard is inconsistent with this Court's "threatened injury" requirement. Respondents' standing theory also rests on a speculative chain of possibilities that does not establish that their potential injury is certainly impending or is fairly traceable to §1881a. First, it is highly speculative whether the Government will imminently target communications to which respondents are parties. Since respondents, as U.S. persons, cannot be targeted under §1881a, their theory necessarily rests on their assertion that their foreign contacts will be targeted. Yet they have no actual knowledge of the Government's §1881a targeting practices. Second, even if respondents could demonstrate that the targeting of their foreign contacts is imminent, they can only speculate as to whether the Government will seek to use §1881a-authorized surveillance instead of one of the Government's numerous other surveillance methods, which are not challenged here. Third, even if respondents could show that the Government will seek FISC authorization to target respondents' foreign contacts under §1881a, they can only speculate as to whether the FISC will authorize the surveillance. This Court is reluctant to endorse standing theories that require guesswork as to how independent decisionmakers will exercise their judgment. See, e.g., Whitmore, supra, at 159–160. Fourth, even if the Government were to obtain the FISC's approval to target respondents' foreign contacts under §1881a, it is unclear whether the Government would succeed in acquiring those contacts' communications. And fifth, even if the Government were to target respondents' foreign contacts, respondents can only speculate as to whether their own communications with those contacts would be incidentally acquired. Pp. 10–15.

(c) Respondents' alternative argument is also unpersuasive. They claim that they suffer ongoing injuries that are fairly traceable to §1881a because the risk of §1881a surveillance requires them to take costly and burdensome measures to protect the confidentiality of their communications. But respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future
Syllabus

harm that is not certainly impending. Because they do not face a threat of certainly impending interception under §1881a, their costs are simply the product of their fear of surveillance, which is insufficient to create standing. See Laird v. Tatum, 408 U. S. 1, 10–15. Accordingly, any ongoing injuries that respondents are suffering are not fairly traceable to §1881a. Pp. 16–20.

(d) Respondents' remaining arguments are likewise unavailing. Contrary to their claim, their alleged injuries are not the same kinds of injuries that supported standing in cases such as Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U. S. 167, Meese v. Keene, 481 U. S. 465, and Monsanto, supra. And their suggestion that they should be held to have standing because otherwise the constitutionality of §1881a will never be adjudicated is both legally and factually incorrect. First, "'[t]he assumption that if respondents have no standing to sue, no one would have standing, is not a reason to find standing.'" Valley Forge Christian College v. Americans United for Separation of Church and State, Inc., 454 U. S. 464, 489. Second, the holding in this case by no means insulates §1881a from judicial review. Pp. 20–23.

638 F. 3d 118, reversed and remanded.

ALITO, J., delivered the opinion of the Court, in which ROBERTS, C. J., and SCALIA, KENNEDY, and THOMAS, JJ., joined. BREYER, J., filed a dissenting opinion, in which GINSBURG, SOTOMAYOR, and KAGAN, JJ., joined.
Opinion of the Court

NOTICE. This opinion is subject to formal revision before publication in the preliminary print of the United States Reports. Readers are requested to notify the Reporter of Decisions, Supreme Court of the United States, Washington, D. C. 20543, of any typographical or other formal errors, in order that corrections may be made before the preliminary print goes to press.

SUPREME COURT OF THE UNITED STATES

No. 11–1025

JAMES R. CLAPPER, JR., DIRECTOR OF NATIONAL INTELLIGENCE, ET AL., PETITIONERS v. AMNESTY INTERNATIONAL USA ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

[February 26, 2013]

JUSTICE ALITO delivered the opinion of the Court.

Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U. S. C. §1881a (2006 ed., Supp. V), allows the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not “United States persons” and are reasonably believed to be located outside the United States. Before doing so, the Attorney General and the Director of National Intelligence normally must obtain the Foreign Intelligence Surveillance Court’s approval. Respondents are United States persons whose work, they allege, requires them to engage in sensitive international communications with individuals who they believe are likely targets of surveillance under §1881a. Respondents seek a declaration that §1881a is unconstitutional, as well as an injunction against §1881a-authorized surveillance. The question

¹The term "United States person" includes citizens of the United States, aliens admitted for permanent residence, and certain associations and corporations. 50 U. S. C. §1801(i); see §1881(a).
before us is whether respondents have Article III standing to seek this prospective relief.

Respondents assert that they can establish injury in fact because there is an objectively reasonable likelihood that their communications will be acquired under §1881a at some point in the future. But respondents' theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be "certainly impending." *E.g.*, *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990). And even if respondents could demonstrate that the threatened injury is certainly impending, they still would not be able to establish that this injury is fairly traceable to §1881a. As an alternative argument, respondents contend that they are suffering present injury because the risk of §1881a-authorized surveillance already has forced them to take costly and burdensome measures to protect the confidentiality of their international communications. But respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending. We therefore hold that respondents lack Article III standing.

A

 Opinion of the Court

when conducting “surveillance of ‘ordinary crime’” might not be required in the context of surveillance conducted for domestic national-security purposes. Id., at 322–323. Although the Keith opinion expressly disclaimed any ruling “on the scope of the President’s surveillance power with respect to the activities of foreign powers,” id., at 308, it implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible, see id., at 322–323.

In constructing such a framework for foreign intelligence surveillance, Congress created two specialized courts. In FISA, Congress authorized judges of the Foreign Intelligence Surveillance Court (FISC) to approve electronic surveillance for foreign intelligence purposes if there is probable cause to believe that “the target of the electronic surveillance is a foreign power or an agent of a foreign power,” and that each of the specific “facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.” §105(a)(3), 92 Stat. 1790; see §§105(b)(1)(A), (b)(1)(B), ibid.; 1 Kris & Wilson §7:2, at 194–195; id., §16:2, at 528–529. Additionally, Congress vested the Foreign Intelligence Surveillance Court of Review with jurisdiction to review any denials by the FISC of applications for electronic surveillance. §103(b), 92 Stat. 1788; 1 Kris & Wilson §5:7, at 151–153.

In the wake of the September 11th attacks, President George W. Bush authorized the National Security Agency (NSA) to conduct warrantless wiretapping of telephone and e-mail communications where one party to the communication was located outside the United States and a participant in “the call was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization,” App. to Pet. for Cert. 403a. See id., at 263a–265a, 268a, 273a–279a, 292a–293a; American Civil Liberties Union v. NSA, 493 F. 3d 644, 648 (CA6 2007)
Opinion of the Court

(ACLU) (opinion of Batchelder, J.). In January 2007, the FISC issued orders authorizing the Government to target international communications into or out of the United States where there was probable cause to believe that one participant to the communication was a member or agent of al Qaeda or an associated terrorist organization. App. to Pet. for Cert. 312a, 398a, 405a. These FISC orders subjected any electronic surveillance that was then occurring under the NSA's program to the approval of the FISC. Id., at 405a; see id., at 312a, 404a. After a FISC Judge subsequently narrowed the FISC's authorization of such surveillance, however, the Executive asked Congress to amend FISA so that it would provide the intelligence community with additional authority to meet the challenges of modern technology and international terrorism. Id., at 315a–318a, 331a–333a, 398a; see id., at 262a, 277a–279a, 287a.

When Congress enacted the FISA Amendments Act of 2008 (FISA Amendments Act), 122 Stat. 2496, it left much of FISA intact, but it "established a new and independent source of intelligence collection authority, beyond that granted in traditional FISA." 1 Kris & Wilson §9:11, at 349–350. As relevant here, §702 of FISA, 50 U.S.C. §1881a (2006 ed., Supp. V), which was enacted as part of the FISA Amendments Act, supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting the communications of non-U.S. persons located abroad. Unlike traditional FISA surveillance, §1881a does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power. Compare §§1805(a)(2)(A), (a)(2)(B), with §§1881a(d)(1), (i)(3)(A); 638 F. 3d 118, 126 (CA2 2011); 1 Kris & Wilson §16:16, at 584. And, unlike traditional FISA, §1881a does not require the
Opinion of the Court

Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur. Compare §§1805(a)(2)(B), (c)(1) (2006 ed. and Supp. V), with §§1881a(d)(1), (g)(4), (i)(3)(A); 638 F. 3d, at 125–126; 1 Kris & Wilson §16:16, at 585.2

The present case involves a constitutional challenge to §1881a. Surveillance under §1881a is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment. Section 1881a provides that, upon the issuance of an order from the Foreign Intelligence Surveillance Court, “the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year . . . , the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” §1881a(a). Surveillance under §1881a may not be intentionally targeted at any person known to be in the United States or any U. S. person reasonably believed to be located abroad. §§1881a(b)(1)–(3); see also §1301(f).

Additionally, acquisitions under §1881a must comport with the Fourth Amendment. §1881a(b)(5). Moreover, surveillance under §1881a is subject to congressional oversight and several types of Executive Branch review. See §§1881a(b)(2), (l); Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633, 640–641 (SDNY 2009).

Section 1881a mandates that the Government obtain the Foreign Intelligence Surveillance Court's approval of “targeting” procedures, “minimization” procedures, and a governmental certification regarding proposed surveillance. §§1881a(a), (c)(1), (i)(2), (i)(3). Among other things, the Government’s certification must attest that (1) procedures are in place “that have been approved, have been submitted for approval, or will be submitted with the

---

2Congress recently reauthorized the FISA Amendments Act for another five years. See 126 Stat. 1631.
Opinion of the Court

certification for approval by the [FISC] that are reasonably designed" to ensure that an acquisition is "limited to targeting persons reasonably believed to be located outside" the United States; (2) minimization procedures adequately restrict the acquisition, retention, and dissemination of nonpublic information about unconsenting U.S. persons, as appropriate; (3) guidelines have been adopted to ensure compliance with targeting limits and the Fourth Amendment; and (4) the procedures and guidelines referred to above comport with the Fourth Amendment. §1881a(g)(2); see §1801(h).

The Foreign Intelligence Surveillance Court's role includes determining whether the Government's certification contains the required elements. Additionally, the Court assesses whether the targeting procedures are "reasonably designed" (1) to "ensure that an acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States" and (2) to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known . . . to be located in the United States." §1881a(i)(2)(B). The Court analyzes whether the minimization procedures "meet the definition of minimization procedures under section 1801(b) . . . , as appropriate." §1881a(i)(2)(C). The Court also assesses whether the targeting and minimization procedures are consistent with the statute and the Fourth Amendment. See §1881a(i)(3)(A).³

³The dissent attempts to downplay the safeguards established by §1881a. See post, at 4 (opinion of BREYER, J.). Notably, the dissent does not directly acknowledge that §1881a surveillance must comport with the Fourth Amendment, see §1881a(b)(5), and that the Foreign Intelligence Surveillance Court must assess whether targeting and minimization procedures are consistent with the Fourth Amendment, see §1881a(i)(3)(A).
Opinion of the Court

B

Respondents are attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad. Respondents believe that some of the people with whom they exchange foreign intelligence information are likely targets of surveillance under §1881a. Specifically, respondents claim that they communicate by telephone and e-mail with people the Government “believes or believed to be associated with terrorist organizations,” “people located in geographic areas that are a special focus” of the Government’s counterterrorism or diplomatic efforts, and activists who oppose governments that are supported by the United States Government. App. to Pet. for Cert. 399a.

Respondents claim that §1881a compromises their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients. Respondents also assert that they “have ceased engaging” in certain telephone and e-mail conversations. Id., at 400a. According to respondents, the threat of surveillance will compel them to travel abroad in order to have in-person conversations. In addition, respondents declare that they have undertaken “costly and burdensome measures” to protect the confidentiality of sensitive communications. Ibid.

C

On the day when the FISA Amendments Act was enacted, respondents filed this action seeking (1) a declaration that §1881a, on its face, violates the Fourth Amendment, the First Amendment, Article III, and separation-of-powers principles and (2) a permanent injunction against the use of §1881a. Respondents assert what they charac-
Opinion of the Court

terize as two separate theories of Article III standing. First, they claim that there is an objectively reasonable likelihood that their communications will be acquired under §1881a at some point in the future, thus causing them injury. Second, respondents maintain that the risk of surveillance under §1881a is so substantial that they have been forced to take costly and burdensome measures to protect the confidentiality of their international communications; in their view, the costs they have incurred constitute present injury that is fairly traceable to §1881a.

After both parties moved for summary judgment, the District Court held that respondents do not have standing. McConnell, 646 F. Supp. 2d, at 635. On appeal, however, a panel of the Second Circuit reversed. The panel agreed with respondents’ argument that they have standing due to the objectively reasonable likelihood that their communications will be intercepted at some time in the future. 638 F. 3d, at 133, 134, 139. In addition, the panel held that respondents have established that they are suffering “present injuries in fact—economic and professional harms—stemming from a reasonable fear of future harmful government conduct.” Id., at 138. The Second Circuit denied rehearing en banc by an equally divided vote. 667 F. 3d 163 (2011).

Because of the importance of the issue and the novel view of standing adopted by the Court of Appeals, we granted certiorari, 566 U. S. ___ (2012), and we now reverse.

II

Article III of the Constitution limits federal courts' jurisdiction to certain “Cases” and “Controversies.” As we have explained, “[n]o principle is more fundamental to the judiciary’s proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.” DaimlerChrysler Corp. v.
Opinion of the Court


The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches. Summers, supra, at 492–493; Daimler-Chrysler Corp., supra, at 341–342, 353; Raines, supra, at 818–820; Valley Forge Christian College v. Americans United for Separation of Church and State, Inc., 454 U. S. 464, 471–474 (1982); Schlesinger v. Reservists Comm. to Stop the War, 418 U. S. 208, 221–222 (1974). In keeping with the purpose of this doctrine, “[o]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional.” Raines, supra, at 819–820; see Valley Forge Christian College, supra, at 473–474; Schlesinger, supra, at 221–222. “Relaxation of standing requirements is directly related to the expansion of judicial power,” United States v. Richardson, 418 U. S. 166, 188 (1974) (Powell, J., concurring); see also Summers, supra, at 492–493; Schlesinger, supra, at 222, and we have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs, see, e.g., Richardson, supra, at 167–170 (plaintiff lacked standing to challenge the constitutionality of a statute permitting the Central Intelligence Agency to account for its expenditures solely on the certificate of the
CIA Director); Schlesinger, supra, at 209–211 (plaintiffs lacked standing to challenge the Armed Forces Reserve membership of Members of Congress); Laird v. Tatum, 408 U.S. 1, 11–16 (1972) (plaintiffs lacked standing to challenge an Army intelligence-gathering program).

To establish Article III standing, an injury must be “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.” Monsanto Co. v. Geertson Seed Farms, 561 U. S. ___ ___ (2010) (slip op., at 7); see also Summers, supra, at 493; Defenders of Wildlife, 504 U. S., at 560–561. “Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is certainly impending.” Id., at 565, n. 2 (internal quotation marks omitted). Thus, we have repeatedly reiterated that “threatened injury must be certainly impending to constitute injury in fact,” and that “[a]llegations of possible future injury” are not sufficient. Whitmore, 495 U. S., at 158 (emphasis added; internal quotation marks omitted); see also Defenders of Wildlife, supra, at 565, n. 2, 567, n. 3; see DaimlerChrysler Corp., supra, at 345; Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U. S. 167, 190 (2000); Babbitt v. Farm Workers, 442 U. S. 289, 298 (1979).

III

A

Respondents assert that they can establish injury in fact that is fairly traceable to §1881a because there is an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted under §1881a at some point in the future. This argument fails. As an initial matter, the Second Circuit’s “objectively reasonable likelihood” standard is inconsistent with our
Opinion of the Court

requirement that "threatened injury must be certainly impending to constitute injury in fact." *Whitmore, supra*, at 158 (internal quotation marks omitted); see also *DaimlerChrysler Corp., supra*, at 345; *Laidlaw, supra*, at 190; *Defenders of Wildlife, supra*, at 565, n. 2; *Babbitt, supra*, at 298. Furthermore, respondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U. S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under §1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy §1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts. As discussed below, respondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending. See *Summers, supra*, at 496 (rejecting a standing theory premised on a speculative chain of possibilities); *Whitmore, supra*, at 157–160 (same). Moreover, even if respondents could demonstrate injury in fact, the second link in the above-described chain of contingencies—which amounts to mere speculation about whether surveillance would be under §1881a or some other authority—shows that respondents cannot satisfy the requirement that any injury in fact must be fairly traceable to §1881a.

First, it is speculative whether the Government will imminently target communications to which respondents are parties. Section 1881a expressly provides that respondents, who are U. S. persons, cannot be targeted for
surveillance under §1881a. See §§1881a(b)(1)–(3); 667 F. 3d, at 173 (Raggi, J., dissenting from denial of rehearing en banc). Accordingly, it is no surprise that respondents fail to offer any evidence that their communications have been monitored under §1881a, a failure that substantially undermines their standing theory. See ACLU, 493 F. 3d, at 655–656, 673–674 (opinion of Batchelder, J.) (concluding that plaintiffs who lacked evidence that their communications had been intercepted did not have standing to challenge alleged NSA surveillance). Indeed, respondents do not even allege that the Government has sought the FISC’s approval for surveillance of their communications. Accordingly, respondents’ theory necessarily rests on their assertion that the Government will target other individuals—notably, their foreign contacts.

Yet respondents have no actual knowledge of the Government’s §1881a targeting practices. Instead, respondents merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired under §1881a. See 667 F. 3d, at 185–187 (opinion of Raggi, J.). For example, journalist Christopher Hedges states: “I have no choice but to assume that any of my international communications may be subject to government surveillance, and I have to make decisions . . . in light of that assumption.” App. to Pet. for Cert. 366a (emphasis added and deleted). Similarly, attorney Scott McKay asserts that, “[b]ecause of the [FISA Amendments Act], we now have to assume that every one of our international communications may be monitored by the government.” Id., at 375a (emphasis added); see also id., at 337a, 343a–344a, 350a, 356a. “The party invoking federal jurisdiction bears the burden of establishing” standing—and, at the summary judgment stage, such a party “can no longer rest on . . . ‘mere allegations,’ but must ‘set forth’ by affidavit or other evidence ‘specific facts.’” Defenders of Wildlife, 504 U. S., at 561. Respondents, however, have
set forth no specific facts demonstrating that the communications of their foreign contacts will be targeted. Moreover, because §1881a at most authorizes—but does not mandate or direct—the surveillance that respondents fear, respondents' allegations are necessarily conjectural. See United Presbyterian Church in U. S. A. v. Reagan, 738 F. 2d 1375, 1380 (CADC 1984) (Scalia, J.); 667 F. 3d, at 187 (opinion of Raggi, J.). Simply put, respondents can only speculate as to how the Attorney General and the Director of National Intelligence will exercise their discretion in determining which communications to target.4

Second, even if respondents could demonstrate that the targeting of their foreign contacts is imminent, respondents can only speculate as to whether the Government will seek to use §1881a-authorized surveillance (rather than other methods) to do so. The Government has numerous other methods of conducting surveillance, none of which is challenged here. Even after the enactment of the FISA Amendments Act, for example, the Government may still conduct electronic surveillance of persons abroad under the older provisions of FISA so long as it satisfies the

4It was suggested at oral argument that the Government could help resolve the standing inquiry by disclosing to a court, perhaps through an in camera proceeding, (1) whether it is intercepting respondents' communications and (2) what targeting or minimization procedures it is using. See Tr. of Oral Arg. 13–14, 44, 56. This suggestion is puzzling. As an initial matter, it is respondents' burden to prove their standing by pointing to specific facts, Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992), not the Government's burden to disprove standing by revealing details of its surveillance priorities. Moreover, this type of hypothetical disclosure proceeding would allow a terrorist (or his attorney) to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program. Even if the terrorist's attorney were to comply with a protective order prohibiting him from sharing the Government's disclosures with his client, the court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets.
applicable requirements, including a demonstration of probable cause to believe that the person is a foreign power or agent of a foreign power. See §1805. The Government may also obtain information from the intelligence services of foreign nations. Brief for Petitioners 33. And, although we do not reach the question, the Government contends that it can conduct FISA-exempt human and technical surveillance programs that are governed by Executive Order 12333. See Exec. Order No. 12333, §§1.4, 2.1–2.5, 3 CFR 202, 210–212 (1981), reprinted as amended, note following 50 U. S. C. §401, pp. 543, 547–548. Even if respondents could demonstrate that their foreign contacts will imminently be targeted—indeed, even if they could show that interception of their own communications will imminently occur—they would still need to show that their injury is fairly traceable to §1881a. But, because respondents can only speculate as to whether any (asserted) interception would be under §1881a or some other authority, they cannot satisfy the "fairly traceable" requirement.

Third, even if respondents could show that the Government will seek the Foreign Intelligence Surveillance Court's authorization to acquire the communications of respondents' foreign contacts under §1881a, respondents can only speculate as to whether that court will authorize such surveillance. In the past, we have been reluctant to endorse standing theories that require guesswork as to how independent decisionmakers will exercise their judgment. In Whitmore, for example, the plaintiff's theory of standing hinged largely on the probability that he would obtain federal habeas relief and be convicted upon retrial. In holding that the plaintiff lacked standing, we explained that "[i]t is just not possible for a litigant to prove in advance that the judicial system will lead to any particular result in his case." 495 U. S., at 159–160; see Defenders of Wildlife, 504 U. S., at 562.
Opinion of the Court

We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors. Section 1881a mandates that the Government must obtain the Foreign Intelligence Surveillance Court’s approval of targeting procedures, minimization procedures, and a governmental certification regarding proposed surveillance. §§1881a(a), (c)(1), (i)(2), (i)(3). The Court must, for example, determine whether the Government’s procedures are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons.” §1801(h); see §§1881a(i)(2), (i)(3)(A). And, critically, the Court must also assess whether the Government’s targeting and minimization procedures comport with the Fourth Amendment. §1881a(i)(3)(A).

Fourth, even if the Government were to obtain the Foreign Intelligence Surveillance Court’s approval to target respondents’ foreign contacts under §1881a, it is unclear whether the Government would succeed in acquiring the communications of respondents’ foreign contacts. And fifth, even if the Government were to conduct surveillance of respondents’ foreign contacts, respondents can only speculate as to whether their own communications with their foreign contacts would be incidentally acquired.

In sum, respondents’ speculative chain of possibilities does not establish that injury based on potential future surveillance is certainly impending or is fairly traceable to §1881a.5

---

5 Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will occur. In some instances, we have found standing based on a "substantial risk" that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm. *Monsanto Co. v. Geertson Seed Farms*, 561 U. S. __, ___ (2010) (slip op., at 11–12). See also *Pennell v. City of San Jose*, 485 U. S. 1, 8 (1988); *Blum v. Yarborough*, 467
Respondents' alternative argument—namely, that they can establish standing based on the measures that they have undertaken to avoid §1881a-authorized surveillance—fares no better. Respondents assert that they are suffering ongoing injuries that are fairly traceable to §1881a because the risk of surveillance under §1881a requires them to take costly and burdensome measures to protect the confidentiality of their communications. Respondents claim, for instance, that the threat of surveillance sometimes compels them to avoid certain e-mail and phone conversations, to “tal[k] in generalities rather than specifics,” or to travel so that they can have in-person conversations. Tr. of Oral Arg. 38; App. to Pet. for Cert. 338a, 345a, 367a, 400a. The Second Circuit panel concluded that, because respondents are already suffering such ongoing injuries, the likelihood of interception under §1881a is relevant only to the question whether respondents' ongoing injuries are “fairly traceable” to §1881a. See

---

U. S. 991, 1000–1001 (1982); Babbitt v. Farm Workers, 442 U. S. 289, 298 (1979). But to the extent that the “substantial risk” standard is relevant and is distinct from the “clearly impending” requirement, respondents fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm here. See supra, at 11–15. In addition, plaintiffs bear the burden of pleading and proving concrete facts showing that the defendant’s actual action has caused the substantial risk of harm. Plaintiffs cannot rely on speculation about “the unfettered choices made by independent actors not before the court.” Defenders of Wildlife, 504 U. S., at 562.

*For all the focus on respondents’ supposed need to travel abroad in light of potential §1881a surveillance, respondents cite only one specific instance of travel: an attorney’s trip to New York City to meet with other lawyers. See App. to Pet. for Cert. 352a. This domestic travel had but a tenuous connection to §1881a, because §1881a-authorized acquisitions “may not intentionally target any person known at the time of acquisition to be located in the United States.” §1881a(b)(1); see also 667 F. 3d 163, 202 (CA2 2011) (Jacobs, C. J., dissenting from denial of rehearing en banc); id., at 185 (opinion of Raggi, J. (same)).
638 F. 3d, at 133–134; 667 F. 3d, at 180 (opinion of Raggi, J.). Analyzing the "fairly traceable" element of standing under a relaxed reasonableness standard, see 638 F. 3d, at 133–134, the Second Circuit then held that "plaintiffs have established that they suffered present injuries in fact—economic and professional harms—stemming from a reasonable fear of future harmful government conduct," id., at 138.

The Second Circuit's analysis improperly allowed respondents to establish standing by asserting that they suffer present costs and burdens that are based on a fear of surveillance, so long as that fear is not "fanciful, paranoid, or otherwise unreasonable." See id., at 134. This improperly waters down the fundamental requirements of Article III. Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending. See Pennsylvania v. New Jersey, 426 U.S. 660, 664 (1976) (per curiam); National Family Planning & Reproductive Health Assn., Inc., 468 F. 3d 826, 831 (CADC 2006). Any ongoing injuries that respondents are suffering are not fairly traceable to §1881a.

If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear. As Judge Raggi accurately noted, under the Second Circuit panel's reasoning, respondents could, "for the price of a plane ticket, . . . transform their standing burden from one requiring a showing of actual or imminent . . . interception to one requiring a showing that their subjective fear of such interception is not fanciful, irrational, or clearly unreasonable." 667 F. 3d, at 180
Opinion of the Court

(internal quotation marks omitted). Thus, allowing respondents to bring this action based on costs they incurred in response to a speculative threat would be tantamount to accepting a repackaged version of respondents' first failed theory of standing. See ACLU, 493 F. 3d, at 656–657 (opinion of Batchelder, J.).

Another reason that respondents' present injuries are not fairly traceable to §1881a is that even before §1881a was enacted, they had a similar incentive to engage in many of the countermeasures that they are now taking. See id., at 668–670. For instance, respondent Scott McKay's declaration describes—and the dissent heavily relies on—Mr. McKay's "knowledge" that thousands of communications involving one of his clients were monitored in the past. App. to Pet. for Cert. 370a; post, at 4, 7–8. But this surveillance was conducted pursuant to FISA authority that predated §1881a. See Brief for Petitioners 32, n. 11; Al-Kidd v. Gonzales, No. 05–cv–93, 2008 WL 5123009 (D Idaho, Dec. 4, 2008). Thus, because the Government was allegedly conducting surveillance of Mr. McKay's client before Congress enacted §1881a, it is difficult to see how the safeguards that Mr. McKay now claims to have implemented can be traced to §1881a.

Because respondents do not face a threat of certainly impending interception under §1881a, the costs that they have incurred to avoid surveillance are simply the product of their fear of surveillance, and our decision in Laird

---

*Although respondents' alternative theory of standing rests primarily on choices that they have made based on their subjective fear of surveillance, respondents also assert that third parties might be disinclined to speak with them due to a fear of surveillance. See App. to Pet. for Cert. 372a–373a, 352a–353a. To the extent that such assertions are based on anything other than conjecture, see Defenders of Wildlife, 504 U.S., at 560, they do not establish injury that is fairly traceable to §1881a, because they are based on third parties' subjective fear of surveillance, see Laird, 408 U. S., at 10–14.*
Opinion of the Court

makes it clear that such a fear is insufficient to create standing. See 408 U. S., at 10–15. The plaintiffs in Laird argued that their exercise of First Amendment rights was being “chilled by the mere existence, without more, of [the Army’s] investigative and data-gathering activity.” Id., at 10. While acknowledging that prior cases had held that constitutional violations may arise from the chilling effect of “regulations that fall short of a direct prohibition against the exercise of First Amendment rights,” the Court declared that none of those cases involved a “chilling effect arising merely from the individual’s knowledge that a governmental agency was engaged in certain activities or from the individual’s concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual.” Id., at 11. Because “[a]llegations of a subjective ‘chill’ are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm,” id., at 13–14, the plaintiffs in Laird—and respondents here—lack standing. See ibid.; ACLU, supra, at 661–662 (opinion of Batchelder, J.) (holding that plaintiffs lacked standing because they “allege[d] only a subjective apprehension” of alleged NSA surveillance and “a personal (self-imposed) unwillingness to communicate”); United Presbyterian Church, 738 F. 2d, at 1378 (holding that plaintiffs lacked standing to challenge the legality of an Executive Order relating to surveillance because “the ‘chilling effect’ which is produced by their fear of being subjected to illegal surveillance and which deters them from conducting constitutionally protected activities, is foreclosed as a basis for standing” by Laird).

For the reasons discussed above, respondents’ self-inflicted injuries are not fairly traceable to the Government’s purported activities under §1881a, and their subjective fear of surveillance does not give rise to standing.
Respondents incorrectly maintain that "[t]he kinds of injuries incurred here—injuries incurred because of [respondents'] reasonable efforts to avoid greater injuries that are otherwise likely to flow from the conduct they challenge—are the same kinds of injuries that this Court held to support standing in cases such as" Laidlaw, Meese v. Keene, 481 U. S. 465 (1987), and Monsanto. Brief for Respondents 24. As an initial matter, none of these cases holds or even suggests that plaintiffs can establish standing simply by claiming that they experienced a "chilling effect" that resulted from a governmental policy that does not regulate, constrain, or compel any action on their part. Moreover, each of these cases was very different from the present case.

In Laidlaw, plaintiffs' standing was based on "the proposition that a company's continuous and pervasive illegal discharges of pollutants into a river would cause nearby residents to curtail their recreational use of that waterway and would subject them to other economic and aesthetic harms." 528 U.S., at 184. Because the unlawful discharges of pollutants were "concededly ongoing," the only issue was whether "nearby residents"—who were members of the organizational plaintiffs—acted reasonably in refraining from using the polluted area. Id., at 183–184. Laidlaw is therefore quite unlike the present case, in which it is not "concede[d]" that respondents would be subject to unlawful surveillance but for their decision to take preventive measures. See ACLU, 493 F. 3d, at 686 (opinion of Batchelder, J.) (distinguishing Laidlaw on this ground); id., at 689–690 (Gibbons, J., concurring) (same); 667 F. 3d, at 182–183 (opinion of Raggi, J.) (same). Laidlaw would resemble this case only if (1) it were undisputed that the Government was using §1881a-authorized surveillance to acquire respondents' communi-
cations and (2) the sole dispute concerned the reasonableness of respondents' preventive measures.

In *Keene*, the plaintiff challenged the constitutionality of the Government's decision to label three films as "political propaganda." 481 U.S., at 467. The Court held that the plaintiff, who was an attorney and a state legislator, had standing because he demonstrated, through "detailed affidavits," that he "could not exhibit the films without incurring a risk of injury to his reputation and of an impairment of his political career." *Id.*, at 467, 473-475. Unlike the present case, *Keene* involved "more than a 'subjective chill'" based on speculation about potential governmental action; the plaintiff in that case was unquestionably regulated by the relevant statute, and the films that he wished to exhibit had already been labeled as "political propaganda." See *ibid.*; *ACLU*, 493 F.3d, at 663-664 (opinion of Breyer, J.); *id.*, at 691 (Gibbons, J., concurring).

*Monsanto*, on which respondents also rely, is likewise inapposite. In *Monsanto*, conventional alfalfa farmers had standing to seek injunctive relief because the agency's decision to deregulate a variety of genetically engineered alfalfa gave rise to a "significant risk of gene flow to non-genetically-engineered varieties of alfalfa." 561 U.S., at ___ (slip op., at 13). The standing analysis in that case hinged on evidence that genetically engineered alfalfa "seed fields [were] currently being planted in all the major alfalfa seed production areas"; the bees that pollinate alfalfa "have a range of at least two to ten miles"; and the alfalfa seed farms were concentrated in an area well within the bees' pollination range. *Id.*, at ___, and n. 3 (slip op., at 11-12, and n. 3). Unlike the conventional alfalfa farmers in *Monsanto*, however, respondents in the present case present no concrete evidence to substantiate their fears, but instead rest on mere conjecture about possible governmental actions.
Opinion of the Court

B

Respondents also suggest that they should be held to have standing because otherwise the constitutionality of §1881a could not be challenged. It would be wrong, they maintain, to "insulate the government's surveillance activities from meaningful judicial review." Brief for Respondents 60. Respondents' suggestion is both legally and factually incorrect. First, "[t]he assumption that if respondents have no standing to sue, no one would have standing, is not a reason to find standing." Valley Forge Christian College, 454 U. S., at 489; Schlesinger, 418 U. S., at 227; see also Richardson, 418 U. S., at 179; Raines, 521 U. S., at 835 (Souter, J., joined by GINSBURG, J., concurring in judgment).

Second, our holding today by no means insulates §1881a from judicial review. As described above, Congress created a comprehensive scheme in which the Foreign Intelligence Surveillance Court evaluates the Government's certifications, targeting procedures, and minimization procedures—including assessing whether the targeting and minimization procedures comport with the Fourth Amendment. §§1881a(a), (c)(1), (i)(2), (i)(3). Any dissatisfaction that respondents may have about the Foreign Intelligence Surveillance Court's rulings—or the congressional delineation of that court's role—is irrelevant to our standing analysis.

Additionally, if the Government intends to use or disclose information obtained or derived from a §1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition. §§1806(c), 1806(e), 1881e(a) (2006 ed. and Supp. V).\(^8\)

\(^8\)The possibility of judicial review in this context is not farfetched. In United States v. Damrah, 412 F. 3d 618 (CA6 2005), for example, the Government made a pretrial disclosure that it intended to use FISA
Opinion of the Court

Thus, if the Government were to prosecute one of respondent-attorney's foreign clients using §1881a-authorized surveillance, the Government would be required to make a disclosure. Although the foreign client might not have a viable Fourth Amendment claim, see, e.g., United States v. Verdugo-Urquidez, 494 U. S. 259, 261 (1990), it is possible that the monitoring of the target's conversations with his or her attorney would provide grounds for a claim of standing on the part of the attorney. Such an attorney would certainly have a stronger evidentiary basis for establishing standing than do respondents in the present case. In such a situation, unlike in the present case, it would at least be clear that the Government had acquired the foreign client's communications using §1881a-authorized surveillance.

Finally, any electronic communications service provider that the Government directs to assist in §1881a surveillance may challenge the lawfulness of that directive before the FISC. §§1881a(h)(4), (6). Indeed, at the behest of a service provider, the Foreign Intelligence Surveillance Court of Review previously analyzed the constitutionality of electronic surveillance directives issued pursuant to a now-expired set of FISA amendments. See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F. 3d 1004, 1006–1016 (2008) (holding that the provider had standing and that the directives were constitutional).

* * *

We hold that respondents lack Article III standing because they cannot demonstrate that the future injury evidence in a prosecution; the defendant (unsuccessfully) moved to suppress the FISA evidence, even though he had not been the target of the surveillance; and the Sixth Circuit ultimately held that FISA's procedures are consistent with the Fourth Amendment. See id., at 622, 623, 625.
Opinion of the Court
they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm. We therefore reverse the judgment of the Second Circuit and remand the case for further proceedings consistent with this opinion.

*It is so ordered.*
BREYER, J., dissenting

SUPREME COURT OF THE UNITED STATES

No. 11–1025

JAMES R. CLAPPER, JR., DIRECTOR OF NATIONAL INTELLIGENCE, ET AL., PETITIONERS v. AMNESTY INTERNATIONAL USA ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

[February 26, 2013]

JUSTICE BREYER, with whom JUSTICE GINSBURG, JUSTICE SOTOMAYOR, and JUSTICE KAGAN join, dissenting.

The plaintiffs’ standing depends upon the likelihood that the Government, acting under the authority of 50 U. S. C. §1881a (2006 ed., Supp. V), will harm them by intercepting at least some of their private, foreign, telephone, or e-mail conversations. In my view, this harm is not “speculative.” Indeed it is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen. This Court has often found the occurrence of similar future events sufficiently certain to support standing. I dissent from the Court’s contrary conclusion.

I

Article III specifies that the “judicial Power” of the United States extends only to actual “Cases” and “Controversies.” §2. It thereby helps to ensure that the legal questions presented to the federal courts will not take the form of abstract intellectual problems resolved in the “rarified atmosphere of a debating society” but instead those questions will be presented “in a concrete factual context conducive to a realistic appreciation of the consequences of judicial action.” Valley Forge Christian College
BREYER, J., dissenting


The Court has recognized that the precise boundaries of the “case or controversy” requirement are matters of “degree . . . not discernible by any precise test.” Ibid. At the same time, the Court has developed a subsidiary set of legal rules that help to determine when the Constitution’s requirement is met. See Lujan, 504 U.S., at 560–561; id., at 583 (Stevens, J., concurring in judgment). Thus, a plaintiff must have “standing” to bring a legal claim. And a plaintiff has that standing, the Court has said, only if the action or omission that the plaintiff challenges has caused, or will cause, the plaintiff to suffer an injury that is “concrete and particularized,” “actual or imminent,” and “redress[able] by a favorable decision.” Id., at 563–561 (internal quotation marks omitted).

No one here denies that the Government’s interception of a private telephone or e-mail conversation amounts to an injury that is “concrete and particularized.” Moreover, the plaintiffs, respondents here, seek as relief a judgment declaring unconstitutional (and enjoining enforcement of) a statutory provision authorizing those interceptions; and, such a judgment would redress the injury by preventing it. Thus, the basic question is whether the injury, i.e., the interception, is “actual or imminent.”

II

A

Since the plaintiffs fear interceptions of a kind authorized by §1881a, it is important to understand just what kind of surveillance that section authorizes. Congress enacted §1881a in 2008, as an amendment to the pre-existing Foreign Intelligence Surveillance Act of 1978, 50
Breyer, J., dissenting

U.S.C. §1801 et seq. Before the amendment, the Act authorized the Government (acting within the United States) to monitor private electronic communications between the United States and a foreign country if (1) the Government’s purpose was, in significant part, to obtain foreign intelligence information (which includes information concerning a “foreign power” or “territory” related to our “national defense” or “security” or the “conduct of . . . foreign affairs”), (2) the Government’s surveillance target was “a foreign power or an agent of a foreign power,” and (3) the Government used surveillance procedures designed to “minimize the acquisition and retention, and prohibit the dissemination, of” any private information acquired about Americans. §§1801(e), (h), 1804(a).

In addition the Government had to obtain the approval of the Foreign Intelligence Surveillance Court. To do so, it had to submit an application describing (1) each “specific target,” (2) the “nature of the information sought,” and (3) the “type of communications or activities to be subjected to the surveillance.” §1804(a). It had to certify that, in significant part, it sought to obtain foreign intelligence information. Ibid. It had to demonstrate probable cause to believe that each specific target was “a foreign power or an agent of a foreign power.” §§1804(a), 1805(a). It also had to describe instance-specific procedures to be used to minimize intrusions upon Americans’ privacy (compliance with which the court subsequently could assess). §§1804(a), 1805(d)(3).

The addition of §1881a in 2008 changed this prior law in three important ways. First, it eliminated the requirement that the Government describe to the court each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized, basis. §1881a(g). Second, it eliminated the requirement that a target be a “foreign power or an agent of a foreign power.”
IBID. Third, it diminished the court's authority to insist upon, and eliminated its authority to supervise, instance-specific privacy-intrusion minimization procedures (though the Government still must use court-approved general minimization procedures). §1881a(e). Thus, using the authority of §1881a, the Government can obtain court approval for its surveillance of electronic communications between places within the United States and targets in foreign territories by showing the court (1) that "a significant purpose of the acquisition is to obtain foreign intelligence information," and (2) that it will use general targeting and privacy-intrusion minimization procedures of a kind that the court had previously approved. §1881a(g).

B

It is similarly important to understand the kinds of communications in which the plaintiffs say they engage and which they believe the Government will intercept. Plaintiff Scott McKay, for example, says in an affidavit (1) that he is a lawyer; (2) that he represented "Mr. Sami Omar Al-Hussayen, who was acquitted in June 2004 on terrorism charges"; (3) that he continues to represent "Mr. Al-Hussayen, who, in addition to facing criminal charges after September 11, was named as a defendant in several civil cases"; (4) that he represents Khalid Sheik Mohammed, a detainee, "before the Military Commissions at Guantánamo Bay, Cuba"; (5) that in representing these clients he "communicate[s] by telephone and email with people outside the United States, including Mr. Al-Hussayen himself," "experts, investigators, attorneys, family members . . . and others who are located abroad"; and (6) that prior to 2008 "the U.S. government had intercepted some 10,000 telephone calls and 20,000 email communications involving [his client] Al-Hussayen." App. to Pet. for Cert. 369a–371a.

Another plaintiff, Sylvia Royce, says in her affidavit (1)
that she is an attorney; (2) that she “represent[s] Mohammedou Ould Salahi, a prisoner who has been held at Guantánamo Bay as an enemy combatant”; (3) that, “[i]n connection with [her] representation of Mr. Salahi, [she] receive[s] calls from time to time from Mr. Salahi’s brother, . . . a university student in Germany”; and (4) that she has been told that the Government has threatened Salahi “that his family members would be arrested and mistreated if he did not cooperate.” *Id.*, at 349a–351a.

The plaintiffs have noted that McKay no longer represents Mohammed and Royce no longer represents Ould Salahi. Brief for Respondents 15, n. 11. But these changes are irrelevant, for we assess standing as of the time a suit is filed, see *Davis v. Federal Election Comm’n*, 554 U. S. 724, 734 (2008), and in any event McKay himself continues to represent Al Hussayen, his partner now represents Mohammed, and Royce continues to represent individuals held in the custody of the U. S. military overseas.

A third plaintiff, Joanne Mariner, says in her affidavit (1) that she is a human rights researcher, (2) that “some of the work [she] do[es] involves trying to track down people who were rendered by the CIA to countries in which they were tortured”; (3) that many of those people “the CIA has said are (or were) associated with terrorist organizations”; and (4) that, to do this research, she “communicate[s] by telephone and e-mail with . . . former detainees, lawyers for detainees, relatives of detainees, political activists, journalists, and fixers” “all over the world, including in Jordan, Egypt, Pakistan, Afghanistan, [and] the Gaza Strip.” App. to Pet. for Cert. 343a–344a.

Other plaintiffs, including lawyers, journalists, and human rights researchers, say in affidavits (1) that they have jobs that require them to gather information from foreigners located abroad; (2) that they regularly communicate electronically (e.g., by telephone or e-mail) with
foreigners located abroad; and (3) that in these communications they exchange “foreign intelligence information” as the Act defines it. *Id.*, at 334a–375a.

III

Several considerations, based upon the record along with commonsense inferences, convince me that there is a very high likelihood that Government, *acting under the authority of §1881a*, will intercept at least some of the communications just described. First, the plaintiffs have engaged, and continue to engage, in electronic communications of a kind that the 2008 amendment, but not the prior Act, authorizes the Government to intercept. These communications include discussions with family members of those detained at Guantanamo, friends and acquaintances of those persons, and investigators, experts and others with knowledge of circumstances related to terrorist activities. These persons are foreigners located outside the United States. They are not “foreign power[s]” or “agent[s] of . . . foreign power[s].” And the plaintiffs state that they exchange with these persons “foreign intelligence information,” defined to include information that “relates to” “international terrorism” and “the national defense or the security of the United States.” See 50 U. S. C. §1801 (2006 ed. and Supp. V); see, *e.g.*, App. to Pet. for Cert. 342a, 366a, 373a–374a.

Second, the plaintiffs have a strong *motive* to engage in, and the Government has a strong *motive* to listen to, conversations of the kind described. A lawyer representing a client normally seeks to learn the circumstances surrounding the crime (or the civil wrong) of which the client is accused. A fair reading of the affidavit of Scott McKay, for example, taken together with elementary considerations of a lawyer’s obligation to his client, indicates that McKay will engage in conversations that concern what suspected foreign terrorists, such as his client,
have done; in conversations that concern his clients' families, colleagues, and contacts; in conversations that concern what those persons (or those connected to them) have said and done, at least in relation to terrorist activities; in conversations that concern the political, social, and commercial environments in which the suspected terrorists have lived and worked; and so forth. See, e.g., id., at 373a–374a. Journalists and human rights workers have strong similar motives to conduct conversations of this kind. See, e.g., id., at 342a (Declaration of Joanne Marinier, stating that “some of the information [she] exchange[s] by telephone and e-mail relates to terrorism and counterterrorism, and much of the information relates to the foreign affairs of the United States”).

At the same time, the Government has a strong motive to conduct surveillance of conversations that contain material of this kind. The Government, after all, seeks to learn as much as it can reasonably learn about suspected terrorists (such as those detained at Guantanamo), as well as about their contacts and activities, along with those of friends and family members. See Executive Office of the President, Office of Management and Budget, Statement of Administration Policy on S. 2248, p. 4 (Dec. 17, 2007) (“Part of the value of the [new authority] is to enable the Intelligence Community to collect expeditiously the communications of terrorists in foreign countries who may contact an associate in the United States”). And the Government is motivated to do so, not simply by the desire to help convict those whom the Government believes guilty, but also by the critical, overriding need to protect America from terrorism. See id., at 1 (“Protection of the American people and American interests at home and abroad requires access to timely, accurate, and insightful intelligence on the capabilities, intentions, and activities of . . . terrorists”).

Third, the Government’s past behavior shows that it has
sought, and hence will in all likelihood continue to seek, information about alleged terrorists and detainees through means that include surveillance of electronic communications. As just pointed out, plaintiff Scott McKay states that the Government (under the authority of the pre-2008 law) "intercepted some 10,000 telephone calls and 20,000 email communications involving [his client] Mr. Al-Hussayen." App. to Pet. for Cert. 370a.

Fourth, the Government has the capacity to conduct electronic surveillance of the kind at issue. To some degree this capacity rests upon technology available to the Government. See 1 D. Kris & J. Wilson, National Security Investigations & Prosecutions §16:6, p. 562 (2d ed. 2012) ("NSA's technological abilities are legendary"); id., §16:12, at 572–577 (describing the National Security Agency's capacity to monitor "very broad facilities" such as international switches). See, e.g., Lichtblau & Risen, Spy Agency Mined Vast Data Trove, Officials Report, N. Y. Times, Dec. 24, 2005, p. A1 (describing capacity to trace and to analyze large volumes of communications into and out of the United States); Lichtblau & Shane, Bush is Pressed Over New Report on Surveillance, N. Y. Times, May 12, 2006, p. A1 (reporting capacity to obtain access to records of many, if not most, telephone calls made in the United States); Priest & Arkin, A Hidden World, Growing Beyond Control, Washington Post, July 19, 2010, p. A1 (reporting that every day, collection systems at the National Security Agency intercept and store 1.7 billion e-mails, telephone calls and other types of communications). Cf. Statement of Administration Policy on S. 2248, supra, at 3 (rejecting a provision of the Senate bill that would require intelligence analysts to count "the number of persons located in the United States whose communications were reviewed" as "impossible to implement" (internal quotation marks omitted)). This capacity also includes the Government's authority to obtain the kind of information here at issue
BREYER, J., dissenting
from private carriers such as AT&T and Verizon. See 50 U. S. C. §1881a(h). We are further told by amici that the Government is expanding that capacity. See Brief for Electronic Privacy Information Center et al. as 22–23 (National Security Agency will be able to conduct surveillance of most electronic communications between domestic and foreign points).

Of course, to exercise this capacity the Government must have intelligence court authorization. But the Government rarely files requests that fail to meet the statutory criteria. See Letter from Ronald Weich, Assistant Attorney General, to Joseph R. Biden, Jr., 1 (Apr. 30, 2012) (In 2011, of the 1,676 applications to the intelligence court, two were withdrawn by the Government, and the remaining 1,674 were approved, 30 with some modification), online at http://www.justice.gov/nsd/foia/foia_library/2011fisa-ltr.pdf. (as visited Feb. 22, 2013, and available in Clerk of Court's case file). As the intelligence court itself has stated, its review under §1881a is “narrowly circumscribed.” In re Proceedings Required by §702(b) of the FISA Amendments Act of 2008, No. Misc. 08–01 (Aug. 17, 2008), p. 3. There is no reason to believe that the communications described would all fail to meet the conditions necessary for approval. Moreover, compared with prior law, §1881a simplifies and thus expedites the approval process, making it more likely that the Government will use §1881a to obtain the necessary approval.

The upshot is that (1) similarity of content, (2) strong motives, (3) prior behavior, and (4) capacity all point to a very strong likelihood that the Government will intercept at least some of the plaintiffs' communications, including some that the 2008 amendment, §1881a, but not the pre-2008 Act, authorizes the Government to intercept.

At the same time, nothing suggests the presence of some special factor here that might support a contrary conclusion. The Government does not deny that it has both the
motive and the capacity to listen to communications of the kind described by plaintiffs. Nor does it describe any system for avoiding the interception of an electronic communication that happens to include a party who is an American lawyer, journalist, or human rights worker. One can, of course, always imagine some special circumstance that negates a virtual likelihood, no matter how strong. But the same is true about most, if not all, ordinary inferences about future events. Perhaps, despite pouring rain, the streets will remain dry (due to the presence of a special chemical). But ordinarily a party that seeks to defeat a strong natural inference must bear the burden of showing that some such special circumstance exists. And no one has suggested any such special circumstance here.

Consequently, we need only assume that the Government is doing its job (to find out about, and combat, terrorism) in order to conclude that there is a high probability that the Government will intercept at least some electronic communication to which at least some of the plaintiffs are parties. The majority is wrong when it describes the harm threatened plaintiffs as "speculative."

IV
A

The majority more plausibly says that the plaintiffs have failed to show that the threatened harm is "certainly impending." Ante, at 10 (internal quotation marks omitted). But, as the majority appears to concede, see ante, at 15–16, and n. 5, certainty is not, and never has been, the touchstone of standing. The future is inherently uncertain. Yet federal courts frequently entertain actions for injunctions and for declaratory relief aimed at preventing future activities that are reasonably likely or highly likely, but not absolutely certain, to take place. And that degree of certainty is all that is needed to support standing here.
BREYER, J., dissenting

The Court's use of the term "certainly impending" is not to the contrary. Sometimes the Court has used the phrase "certainly impending" as if the phrase described a sufficient, rather than a necessary, condition for jurisdiction. See Pennsylvania v. West Virginia, 262 U.S. 553, 593 (1923) ("If the injury is certainly impending that is enough"). See also Babbitt, 442 U.S., at 298 (same). On other occasions, it has used the phrase as if it concerned when, not whether, an alleged injury would occur. Thus, in Lujan, 504 U.S., at 564, n. 2, the Court considered a threatened future injury that consisted of harm that plaintiffs would suffer when they "soon" visited a government project area that (they claimed) would suffer environmental damage. The Court wrote that a "mere profession of an intent, some day, to return" to the project area did not show the harm was "imminent," for "soon" might mean nothing more than "in this lifetime." Id., at 564–565, n. 2 (internal quotation marks omitted). Similarly, in McConnell v. Federal Election Comm'n, 540 U.S. 93 (2003), the Court denied standing because the Senator's future injury (stemming from a campaign finance law) would not affect him until his reelection. That fact, the Court said, made the injury "too remote temporally to satisfy Article III standing." Id., at 225–226.

On still other occasions, recognizing that "'imminence' is concededly a somewhat elastic concept," Lujan, supra, at 565, n. 2, the Court has referred to, or used (sometimes along with "certainly impending") other phrases such as "reasonable probability" that suggest less than absolute, or literal certainty. See Babbitt, supra, at 298 (plaintiff "must demonstrate a realistic danger of sustaining a direct injury" (emphasis added)); Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167, 190 (2000) ("[I]t is the plaintiff's burden to establish standing by demonstrating that . . . the defendant's allegedly wrongful behavior will likely occur or continue"). See

B

1

More important, the Court’s holdings in standing cases show that standing exists here. The Court has often found standing where the occurrence of the relevant injury was far less certain than here. Consider a few, fairly typical, cases. Consider *Pennell*, supra. A city ordinance forbade landlords to raise the rent charged to a tenant by more than 8 percent where doing so would work an unreasonably severe hardship on that tenant. *Id.*, at 4–5. A group of landlords sought a judgment declaring the ordinance unconstitutional. The Court held that, to have standing, the landlords had to demonstrate a "realistic danger of sustaining a direct injury as a result of the statute's operation." *Id.*, at 8 (emphasis added). It found that the landlords had done so by showing a likelihood of enforcement and a "probability," *ibid.*, that the ordinance would make
the landlords charge lower rents—even though the landlords had not shown (1) that they intended to raise the relevant rents to the point of causing unreasonably severe hardship; (2) that the tenants would challenge those increases; or (3) that the city’s hearing examiners and arbitrators would find against the landlords. Here, even more so than in Pennell, there is a “realistic danger” that the relevant harm will occur.

Or, consider Blum, supra. A group of nursing home residents receiving Medicaid benefits challenged the constitutionality (on procedural grounds) of a regulation that permitted their nursing home to transfer them to a less desirable home. Id., at 999–1000. Although a Medicaid committee had recommended transfers, Medicaid-initiated transfer had been enjoined and the nursing home itself had not threatened to transfer the plaintiffs. But the Court found “standing” because “the threat of transfers” was “not ‘imaginary or speculative’” but “quite realistic,” hence “sufficiently substantial.” Id., at 1000–1001 (quoting Younger v. Harris, 401 U. S. 37, 42 (1971)). The plaintiffs’ injury here is not imaginary or speculative, but “quite realistic.”

Or, consider Davis, supra. The plaintiff, a candidate for the United States House of Representatives, self-financed his campaigns. He challenged the constitutionality of an election law that relaxed the limits on an opponent’s contributions when a self-financed candidate’s spending itself exceeded certain other limits. His opponent, in fact, had decided not to take advantage of the increased contribution limits that the statute would have allowed. Id., at 734. But the Court nonetheless found standing because there was a “realistic and impending threat,” not a certainty, that the candidate’s opponent would do so at the time the plaintiff filed the complaint. Id., at 734–735. The threat facing the plaintiffs here is as “realistic and impending.”
Or, consider *MedImmune*, *supra*. The plaintiff, a patent licensee, sought a declaratory judgment that the patent was invalid. But, the plaintiff did not face an imminent threat of suit because it continued making royalty payments to the patent holder. In explaining why the plaintiff had standing, we (1) assumed that if the plaintiff stopped making royalty payments it would have standing (despite the fact that the patent holder might not bring suit), (2) rejected the Federal Circuit’s “reasonable apprehension of imminent suit” requirement, and (3) instead suggested that a “genuine threat of enforcement” was likely sufficient. *Id.*, at 128, 129, 132, n. 11 (internal quotation marks omitted). A “genuine threat” is present here.

Moreover, courts have often found probabilistic injuries sufficient to support standing. In *Duke Power Co. v. Carolina Environmental Study Group, Inc.*, 438 U. S. 59 (1978), for example, the plaintiffs, a group of individuals living near a proposed nuclear powerplant, challenged the constitutionality of the Price-Anderson Act, a statute that limited the plant’s liability in the case of a nuclear accident. The plaintiffs said that, without the Act, the defendants would not build a nuclear plant. And the building of the plant would harm them, in part, by emitting “non-natural radiation into [their] environment.” *Id.*, at 74. The Court found standing in part due to “our generalized concern about exposure to radiation and the apprehension flowing from the uncertainty about the health and genetic consequences of even small emissions.” *Ibid.* (emphasis added). See also *Monsanto Co.*, *supra*, at ___ (slip op., at 11–12) (“A substantial risk of gene flow injures respondents in several ways” (emphasis added)).

See also lower court cases, such as *Mountain States Legal Foundation v. Glickman*, 92 F. 3d 1228, 1234–1235 (CADC 1996) (plaintiffs attack Government decision to limit timber harvesting; standing based upon increased
risk of wildfires); Natural Resources Defense Council v. EPA, 464 F. 3d 1, 7 (CADC 2006) (plaintiffs attack Government decision deregulating methyl bromide; standing based upon increased lifetime risk of developing skin cancer); Constellation Energy Commodities Group, Inc. v. FERC, 457 F. 3d 14, 20 (CADC 2006) (standing based on increased risk of nonrecovery inherent in the reduction of collateral securing a debt of uncertain amount); Sutton v. St. Jude Medical S. C., Inc., 419 F. 3d 568, 570–575 (CA6 2005) (standing based on increased risk of harm caused by implantation of defective medical device); Johnson v. Allsteel, Inc., 259 F. 3d 885, 888–891 (CA7 2001) (standing based on increased risk that Employee Retirement Income Security Act beneficiary will not be covered due to increased amount of discretion given to ERISA administrator).

How could the law be otherwise? Suppose that a federal court faced a claim by homeowners that (allegedly) unlawful dam-building practices created a high risk that their homes would be flooded. Would the court deny them standing on the ground that the risk of flood was only 60, rather than 90, percent?

Would federal courts deny standing to a plaintiff in a diversity action who claims an anticipatory breach of contract where the future breach depends on probabilities? The defendant, say, has threatened to load wheat onto a ship bound for India despite a promise to send the wheat to the United States. No one can know for certain that this will happen. Perhaps the defendant will change his mind; perhaps the ship will turn and head for the United States. Yet, despite the uncertainty, the Constitution does not prohibit a federal court from hearing such a claim. See 23 R. Lord, Williston on Contracts §63:35 (4th ed. 2002) (plaintiff may bring an anticipatory breach suit even though the defendant's promise is one to perform in the future, it has not yet been broken, and defendant may still
Breyer, J., dissenting


Would federal courts deny standing to a plaintiff who seeks to enjoin as a nuisance the building of a nearby pond which, the plaintiff believes, will very likely, but not inevitably, overflow his land? See 42 Am. Jur. 2d Injunctions §§2, 5 (2010) (noting that an injunction is ordinarily preventive in character and restrains actions that have not yet been taken, but threaten injury). E.g., Central Delta Water Agency v. United States, 306 F. 3d 938, 947–950 (CA9 2002) (standing to seek injunction where method of operating dam was highly likely to severely hamper plaintiffs’ ability to grow crops); Consolidated Companies, Inc. v. Union Pacific R. Co., 499 F. 3d 382, 386 (CA5 2007) (standing to seek injunction requiring cleanup of land adjacent to plaintiff’s tract because of threat that contaminants might migrate to plaintiff’s tract).

Neither do ordinary declaratory judgment actions always involve the degree of certainty upon which the Court insists here. See, e.g., Maryland Casualty Co. v. Pacific Coal & Oil Co., 312 U. S. 270, 273 (1941) (insurance company could seek declaration that it need not pay claim against insured automobile driver who was in an accident even though the driver had not yet been found liable for the accident); Aetna Life Ins. Co. v. Haworth, 300 U. S. 227, 239–244 (1937) (insurance company could seek declaration that it need not pay plaintiff for disability although plaintiff had not yet sought disability payments). See also, e.g., Associated Indemnity Corp. v. Fairchild Industries, Inc., 961 F. 2d 32, 35–36 (CA2 1992) (insured could seek declaration that insurance company must pay liabil-
ity even before insured found liable).

2

In some standing cases, the Court has found that a reasonable probability of future injury comes accompanied with present injury that takes the form of reasonable efforts to mitigate the threatened effects of the future injury or to prevent it from occurring. Thus, in Monsanto Co., 561 U. S., at ___ (slip op., at 11–14) plaintiffs, a group of conventional alfalfa growers, challenged an agency decision to deregulate genetically engineered alfalfa. They claimed that deregulation would harm them because their neighbors would plant the genetically engineered seed, bees would obtain pollen from the neighbors’ plants, and the bees would then (harmfully) contaminate their own conventional alfalfa with the genetically modified gene. The lower courts had found a “reasonable probability” that this injury would occur. Ibid. (internal quotation marks omitted).

Without expressing views about that probability, we found standing because the plaintiffs would suffer present harm by trying to combat the threat. Ibid. The plaintiffs, for example, “would have to conduct testing to find out whether and to what extent their crops have been contaminated.” Id., at ___ (slip op., at 12). And they would have to take “measures to minimize the likelihood of potential contamination and to ensure an adequate supply of non-genetically-engineered alfalfa.” Ibid. We held that these harms, which [the plaintiffs] will suffer even if their crops are not actually infected with” the genetically modified gene, “are sufficiently concrete to satisfy the injury-in-fact prong of the constitutional standing analysis.” Id., at ___ (slip op., at 13).

Virtually identical circumstances are present here. Plaintiff McKay, for example, points out that, when he communicates abroad about, or in the interests of, a client
(e.g., a client accused of terrorism), he must "make an assessment" whether his "client's interests would be compromised" should the Government "acquire the communications." App. to Pet. for Cert. 375a. If so, he must either forgo the communication or travel abroad. Id., at 371a–372a ("I have had to take measures to protect the confidentiality of information that I believe is particularly sensitive," including "travel that is both time-consuming and expensive").

Since travel is expensive, since forgoing communication can compromise the client's interests, since McKay's assessment itself takes time and effort, this case does not differ significantly from Monsanto. And that is so whether we consider the plaintiffs' present necessary expenditure of time and effort as a separate concrete, particularized, imminent harm, or consider it as additional evidence that the future harm (an interception) is likely to occur. See also Friends of the Earth, Inc., 528 U. S., at 183–184 (holding that plaintiffs who curtailed their recreational activities on a river due to reasonable concerns about the effect of pollutant discharges into that river had standing); Meese v. Keene, 481 U. S. 465, 475 (1987) (stating that "the need to take...affirmative steps to avoid the risk of harm...constitutes a cognizable injury").

The majority cannot find support in cases that use the words "certainly impending" to deny standing. While I do not claim to have read every standing case, I have examined quite a few, and not yet found any such case. The majority refers to Whitmore v. Arkansas, 495 U. S. 149 (1990). But in that case the Court denied standing to a prisoner who challenged the validity of a death sentence given to a different prisoner who refused to challenge his own sentence. The plaintiff feared that in the absence of an appeal, his fellow prisoner's death sentence would be
missing from the State's death penalty database and thereby skew the database against him, making it less likely his challenges to his own death penalty would succeed. The Court found no standing. Id., at 161. But the fellow prisoner's lack of appeal would have harmed the plaintiff only if (1) the plaintiff separately obtained federal habeas relief and was then reconvicted and resentenced to death, (2) he sought review of his new sentence, and (3) during that review, his death sentence was affirmed only because it was compared to an artificially skewed database. Id., at 156–157. These events seemed not very likely to occur.

In *DaimlerChrysler Corp. v. Cuno*, 547 U. S. 332 (2006), taxpayers challenged the constitutionality of a tax break offered by state and local governments to a car manufacturer. We found no standing. But the plaintiffs would have suffered resulting injury only if that the tax break had depleted state and local treasuries and the legislature had responded by raising their taxes. Id., at 344.

In *Lujan*, the case that may come closest to supporting the majority, the Court also found no standing. But, as I pointed out, *supra*, at 11, *Lujan* is a case where the Court considered when, not whether, the threatened harm would occur. 504 U. S., at 564, n. 2. The relevant injury there consisted of a visit by environmental group's members to a project site where they would find (unlawful) environmental deprevation. Id., at 564. The Court pointed out that members had alleged that they would visit the project sites "soon." But it wrote that "soon" might refer to almost any time in the future. Ibid., n. 2. By way of contrast, the ongoing threat of terrorism means that here the relevant intercpections will likely take place imminently, if not now.

The Court has, of course, denied standing in other cases. But they involve injuries less likely, not more likely, to occur than here. In a recent case, *Summers v. Earth Island Institute*, 555 U. S. 488 (2009), for example, the
plaintiffs challenged a regulation exempting certain timber sales from public comment and administrative appeal. The plaintiffs claimed that the regulations injured them by interfering with their esthetic enjoyment and recreational use of the forests. The Court found this harm too unlikely to occur to support standing. *Id.*, at 496. The Court noted that one plaintiff had not pointed to a specific affected forest that he would visit. The Court concluded that "[t]here may be a chance, but . . . hardly a likelihood," that the plaintiff's "wanderings will bring him to a parcel about to be affected by a project unlawfully subject to the regulations." *Id.*, at 495 (emphasis added).

4

In sum, as the Court concedes, see *ante*, at 15–16, and n. 5, the word "certainly" in the phrase "certainly impending" does not refer to absolute certainty. As our case law demonstrates, what the Constitution requires is something more akin to "reasonable probability" or "high probability." The use of some such standard is all that is necessary here to ensure the actual concrete injury that the Constitution demands. The considerations set forth in Parts II and III, *supra*, make clear that the standard is readily met in this case.

* * *

While I express no view on the merits of the plaintiffs' constitutional claims, I do believe that at least some of the plaintiffs have standing to make those claims. I dissent, with respect, from the majority's contrary conclusion.
Panel II:

Legislative Updates on Developments in National Security Law

Moderator:
Benjamin Powell
H.R. 1960—FY14 NATIONAL DEFENSE AUTHORIZATION BILL

CHAIRMAN'S MARK

SUMMARY OF BILL LANGUAGE.................................................. 1
BILL LANGUAGE........................................................................... 49
DIRECTIVE REPORT LANGUAGE................................................ 389
Subtitle E—Sensitive Military Operations

SEC. 1041 [Log 51011]. CONGRESSIONAL NOTIFICATION OF SENSITIVE MILITARY OPERATIONS.

(a) Notification Required.—

(1) In general.—Chapter 3 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 130f. Congressional notification of sensitive military operations

(a) In general.—The Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of any sensitive military operation following such operation.

(b) Procedures.—(1) The Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirements of subsection (a) consistent with the national security of the United States and the protection of operational integrity.

(2) The congressional defense committees shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to pro-
tect the information that is submitted to the committees
pursuant to this section.

“(e) SENSITIVE MILITARY OPERATION DEFINED.—
The term ‘sensitive military operation’ means a lethal op-
eration or capture operation conducted by the armed
forces outside the United States pursuant to—

“(1) the Authorization for Use of Military
Force (Public Law 107–40; 50 U.S.C. 1541 note);

or

“(2) any other authority except—

“(A) a declaration of war; or

“(B) a specific statutory authorization for
the use of force other than the authorization re-
ferred to in paragraph (1).

“(d) EXCEPTION.—The notification requirement
under subsection (a) shall not apply with respect to a sen-
sitive military operation executed within the territory of
Afghanistan pursuant to the Authorization for Use of
Military Force (Public Law 107–40; 50 U.S.C. 1541
note).

“(e) RULE OF CONSTRUCTION.—Nothing in this sec-
tion shall be construed to provide any new authority or
to alter or otherwise affect the War Powers Resolution (50
U.S.C. 1541 et seq.), the Authorization for Use of Military
Force (Public Law 107–40; 50 U.S.C. 1541 note), or any
requirement under the National Security Act of 1947 (50
U.S.C. 3001 et seq.)."

(2) CLERICAL AMENDMENT.—The table of sec-

ions at the beginning of such chapter is amended
by inserting after the item relating to section 130e
the following new item:

"130f. Congressional notification regarding sensitive military operations."

(b) EFFECTIVE DATE.—Section 130f of title 10,
United States Code, as added by subsection (a), shall
apply with respect to any sensitive military operation (as
defined in subsection (c) of such section) executed on or
after the date of the enactment of this Act.

(c) DEADLINE FOR SUBMITTAL OF PROCEDURES.—
The Secretary of Defense shall submit to the congressional
defense committees the procedures required under section
130f(b) of title 10, United States Code, as added by sub-
section (a), by not later than 60 days after the date of
the enactment of this Act.
SEC. 1042 [Log 51012]. REPORT ON PROCESS FOR DETERMINING TARGETS OF LETHAL OPERATIONS.

Not later than 60 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report containing an explanation of the legal and policy considerations and approval processes used in determining whether an individual or group of individuals could be the target of a lethal operation or capture operation conducted by the Armed Forces of the United States outside the United States.
SEC. 1043 [Log 51013]. COUNTERTERRORISM OPERATIONAL
BRIEFINGS.

(a) BRIEFINGS REQUIRED.—Chapter 23 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 492. Quarterly briefings: counterterrorism operations

(a) BRIEFINGS REQUIRED.—The Secretary of Defense shall provide to the congressional defense committees quarterly briefings outlining Department of Defense counterterrorism operations and related activities.

(b) ELEMENTS.—Each briefing under subsection (a) shall include each of the following:

"(1) A global update on activity within each geographic combatant command.

"(2) An overview of authorities and legal issues including limitations.

"(3) An outline of interagency activities and initiatives.

"(4) Any other matters the Secretary considers appropriate."

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by adding at the end the following new item:

"492. Quarterly briefings: counterterrorism operations."
Effective: [See Text Amendments]

United States Code Annotated Currentness
Title 50. War and National Defense (Refs & Annos)
   *-* Chapter 33. War Powers Resolution (Refs & Annos)
       ➔ ➔ § 1541. Purpose and policy

(a) Congressional declaration

It is the purpose of this chapter to fulfill the intent of the framers of the Constitution of the United States and in- sure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indi- cated by the circumstances, and to the continued use of such forces in hostilities or in such situations.

(b) Congressional legislative power under necessary and proper clause

Under article I, section 8, of the Constitution, it is specifically provided that the Congress shall have the power to make all laws necessary and proper for carrying into execution, not only its own powers but also all other powers vested by the Constitution in the Government of the United States, or in any department or officer there- of.

(c) Presidential executive power as Commander-in-Chief; limitation

The constitutional powers of the President as Commander-in-Chief to introduce United States Armed Forces in- to hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circum- stances, are exercised only pursuant to (1) a declaration of war, (2) specific statutory authorization, or (3) a na- tional emergency created by attack upon the United States, its territories or possessions, or its armed forces.

CREDIT(S)


HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports


Effective:[See Text Amendments]

United States Code Annotated Currentness
   Title 50. War and National Defense (Refs & Annos)
   ☞ Chapter 33. War Powers Resolution (Refs & Annos)
      ☞ ☞ § 1542. Consultation; initial and regular consultations

The President in every possible instance shall consult with Congress before introducing United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and after every such introduction shall consult regularly with the Congress until United States Armed Forces are no longer engaged in hostilities or have been removed from such situations.

CREDIT(S)


HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports


Effective and Applicability Provisions


LIBRARY REFERENCES

American Digest System

   War and National Emergency ☞ ☞ 37.
   Key Number System Topic No. 402.

RESEARCH REFERENCES

Encyclopedias

Effective:[See Text Amendments]

United States Code Annotated Currentness
Title 50. War and National Defense (Refs & Annos)
  Chapter 33. War Powers Resolution (Refs & Annos)
  § 1543. Reporting requirement

(a) Written report; time of submission; circumstances necessitating submission; information reported

In the absence of a declaration of war, in any case in which United States Armed Forces are introduced--

(1) into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances;

(2) into the territory, airspace or waters of a foreign nation, while equipped for combat, except for deployments which relate solely to supply, replacement, repair, or training of such forces; or

(3) in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a foreign nation;

the President shall submit within 48 hours to the Speaker of the House of Representatives and to the President pro tempore of the Senate a report, in writing, setting forth--

(A) the circumstances necessitating the introduction of United States Armed Forces;

(B) the constitutional and legislative authority under which such introduction took place; and

(C) the estimated scope and duration of the hostilities or involvement.

(b) Other information reported

The President shall provide such other information as the Congress may request in the fulfillment of its constitutional responsibilities with respect to committing the Nation to war and to the use of United States Armed Forces abroad.

(c) Periodic reports; semiannual requirement

Whenever United States Armed Forces are introduced into hostilities or into any situation described in subsection (a) of this section, the President shall, so long as such armed forces continue to be engaged in such hostilities or situation, report to the Congress periodically on the status of such hostilities or situation as well as on the scope and duration of such hostilities or situation, but in no event shall he report to the Congress less often than once every six months.

CREDIT(S)


HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports


Effective and Applicability Provisions


Termination of Reporting Requirements


LAW REVIEW COMMENTARIES


Resolving challenges to statutes containing unconstitutional legislative veto provisions. 85 Colum.L.Rev. 1808 (1985).

Rethinking the role of the war powers resolution: Congress and the Persian Gulf War. Eileen Burgin, 21 J.Legis. 23 (1995).

The war powers resolution: Congress seeks to reassert its proper constitutional role as a partner in war

Effective:[See Text Amendments]

United States Code Annotated Currentness
Title 50. War and National Defense (Refs & Annos)
   ☞ Chapter 33. War Powers Resolution (Refs & Annos)
   ⇌ § 1544. Congressional action

(a) Transmittal of report and referral to Congressional committees; joint request for convening Congress

Each report submitted pursuant to section 1543(a)(1) of this title shall be transmitted to the Speaker of the House of Representatives and to the President pro tempore of the Senate on the same calendar day. Each report so transmitted shall be referred to the Committee on Foreign Affairs of the House of Representatives and to the Committee on Foreign Relations of the Senate for appropriate action. If, when the report is transmitted, the Congress has adjourned sine die or has adjourned for any period in excess of three calendar days, the Speaker of the House of Representatives and the President pro tempore of the Senate, if they deem it advisable (or if petitioned by at least 30 percent of the membership of their respective Houses) shall jointly request the President to convene Congress in order that it may consider the report and take appropriate action pursuant to this section.

(b) Termination of use of United States Armed Forces; exceptions; extension period

Within sixty calendar days after a report is submitted or is required to be submitted pursuant to section 1543(a)(1) of this title, whichever is earlier, the President shall terminate any use of United States Armed Forces with respect to which such report was submitted (or required to be submitted), unless the Congress (1) has declared war or has enacted a specific authorization for such use of United States Armed Forces, (2) has extended by law such sixty-day period, or (3) is physically unable to meet as a result of an armed attack upon the United States. Such sixty-day period shall be extended for not more than an additional thirty days if the President determines and certifies to the Congress in writing that unavoidable military necessity respecting the safety of United States Armed Forces requires the continued use of such armed forces in the course of bringing about a prompt removal of such forces.

(c) Concurrent resolution for removal by President of United States Armed Forces

Notwithstanding subsection (b) of this section, at any time that United States Armed Forces are engaged in hostilities outside the territory of the United States, its possessions and territories without a declaration of war or specific statutory authorization, such forces shall be removed by the President if the Congress so directs by concurrent resolution.
CREDIT(S)


UNCONSTITUTIONALITY OF LEGISLATIVE VETO PROVISIONS

The provisions of former section 1254(c)(2) of Title 8, Aliens and Nationality, which authorized a House of Congress, by resolution, to invalidate an action of the Executive Branch, were declared unconstitutional in Immigration and Naturalization Service v. Chadha, 1983, 103 S.Ct. 2764, 462 U.S. 919, 77 L.Ed.2d 317. See similar provisions in this section.

HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports


Effective and Applicability Provisions


Change of Name

Any reference in any provision of law enacted before Jan. 4, 1995, to the Committee on Foreign Affairs of the House of Representatives treated as referring to the Committee on International Relations of the House of Representatives, see section 1(a)(5) of Pub.L. 104-14, set out as a note preceding section 21 of Title 2, The Congress.

LAW REVIEW COMMENTARIES


Resolving challenges to statutes containing unconstitutional legislative veto provisions. 85 Colum.L.Rev. 1808 (1985).

Rethinking the role of the war powers resolution: Congress and the Persian Gulf War. Eileen Burgin, 21 J.Legis. 23 (1995).

LIBRARY REFERENCES
Effective:[See Text Amendments]

United States Code Annotated Currentness
Title 50. War and National Defense (Refs & Annos)
    Chapter 33. War Powers Resolution (Refs & Annos)
    § 1545. Congressional priority procedures for joint resolution or bill

(a) Time requirement; referral to Congressional committee; single report

Any joint resolution or bill introduced pursuant to section 1544(b) of this title at least thirty calendar days before the expiration of the sixty-day period specified in such section shall be referred to the Committee on Foreign Affairs of the House of Representatives or the Committee on Foreign Relations of the Senate, as the case may be, and such committee shall report one such joint resolution or bill, together with its recommendations, not later than twenty-four calendar days before the expiration of the sixty-day period specified in such section, unless such House shall otherwise determine by the yeas and nays.

(b) Pending business; vote

Any joint resolution or bill so reported shall become the pending business of the House in question (in the case of the Senate the time for debate shall be equally divided between the proponents and the opponents), and shall be voted on within three calendar days thereafter, unless such House shall otherwise determine by yeas and nays.

(c) Referral to other House committee

Such a joint resolution or bill passed by one House shall be referred to the committee of the other House named in subsection (a) of this section and shall be reported out not later than fourteen calendar days before the expiration of the sixty-day period specified in section 1544(b) of this title. The joint resolution or bill so reported shall become the pending business of the House in question and shall be voted on within three calendar days after it has been reported, unless such House shall otherwise determine by yeas and nays.

(d) Disagreement between Houses

In the case of any disagreement between the two Houses of Congress with respect to a joint resolution or bill passed by both Houses, conferees shall be promptly appointed and the committee of conference shall make and file a report with respect to such resolution or bill not later than four calendar days before the expiration of the sixty-day period specified in section 1544(b) of this title. In the event the conferees are unable to agree within
48 hours, they shall report back to their respective Houses in disagreement. Notwithstanding any rule in either House concerning the printing of conference reports in the Record or concerning any delay in the consideration of such reports, such report shall be acted on by both Houses not later than the expiration of such sixty-day period.

CREDIT(S)


UNCONSTITUTIONALITY OF LEGISLATIVE VETO PROVISIONS

The provisions of former section 1254(c)(2) of Title 8, Aliens and Nationality, which authorized a House of Congress, by resolution, to invalidate an action of the Executive Branch, were declared unconstitutional in Immigration and Naturalization Service v. Chadha, 1983, 103 S.Ct. 2764, 462 U.S. 919, 77 L.Ed.2d 317. See similar provisions in this section.

HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports


Effective and Applicability Provisions


Change of Name

Any reference in any provision of law enacted before Jan. 4, 1995, to the Committee on Foreign Affairs of the House of Representatives treated as referring to the Committee on International Relations of the House of Representatives, see section 1(a)(5) of Pub.L. 104-14, set out as a note preceding section 21 of Title 2, The Congress.

LIBRARY REFERENCES

American Digest System

United States 35.
Key Number System Topic No. 393.
Effective:[See Text Amendments]

United States Code Annotated Currentness
Title 50. War and National Defense (Refs & Annos)
→ Chapter 33. War Powers Resolution (Refs & Annos)
⇒ § 1546. Congressional priority procedures for concurrent resolution

(a) Referral to Congressional committee; single report

Any concurrent resolution introduced pursuant to section 1544(c) of this title shall be referred to the Committee on Foreign Affairs of the House of Representatives or the Committee on Foreign Relations of the Senate, as the case may be, and one such concurrent resolution shall be reported out by such committee together with its recommendations within fifteen calendar days, unless such House shall otherwise determine by the yeas and nays.

(b) Pending business; vote

Any concurrent resolution so reported shall become the pending business of the House in question (in the case of the Senate the time for debate shall be equally divided between the proponents and the opponents) and shall be voted on within three calendar days thereafter, unless such House shall otherwise determine by yeas and nays.

(c) Referral to other House committee

Such a concurrent resolution passed by one House shall be referred to the committee of the other House named in subsection (a) of this section and shall be reported out by such committee together with its recommendations within fifteen calendar days and shall thereupon become the pending business of such House and shall be voted upon within three calendar days, unless such House shall otherwise determine by yeas and nays.

(d) Disagreement between Houses

In the case of any disagreement between the two Houses of Congress with respect to a concurrent resolution passed by both Houses, conferees shall be promptly appointed and the committee of conference shall make and file a report with respect to such concurrent resolution within six calendar days after the legislation is referred to the committee of conference. Notwithstanding any rule in either House concerning the printing of conference reports in the Record or concerning any delay in the consideration of such reports, such report shall be acted on by both Houses not later than six calendar days after the conference report is filed. In the event the conferees are unable to agree within 48 hours, they shall report back to their respective Houses in disagreement.
CREDIT(S)


UNCONSTITUTIONALITY OF LEGISLATIVE VETO PROVISIONS

<The provisions of former section 1254(c)(2) of Title 8, Aliens and Nationality, which authorized a House of Congress, by resolution, to invalidate an action of the Executive Branch, were declared unconstitutional in Immigration and Naturalization Service v. Chadha, 1983, 103 S.Ct. 2764, 462 U.S. 919, 77 L.Ed.2d 317. See similar provisions in this section.>

HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports


Effective and Applicability Provisions


Change of Name

Any reference in any provision of law enacted before Jan. 4, 1995, to the Committee on Foreign Affairs of the House of Representatives treated as referring to the Committee on International Relations of the House of Representatives, see section 1(a)(5) of Pub.L. 104-14, set out as a note preceding section 21 of Title 2, The Congress.

LIBRARY REFERENCES

American Digest System

War and National Emergency \(\text{\texttrade} 35.
Key Number System Topic No. 402.

50 U.S.C.A. § 1546, 50 USCA § 1546

Current through P.L. 113-36 approved 9-18-13

Westlaw. (C) 2013 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

Effective:[See Text Amendments]

United States Code Annotated Currentness
Title 50. War and National Defense (Refs & Annos)

mighty Chapter 33. War Powers Resolution (Refs & Annos)
⇒⇒ § 1547. Interpretation of joint resolution

(a) Inferences from any law or treaty

Authority to introduce United States Armed Forces into hostilities or into situations wherein involvement in hostilities is clearly indicated by the circumstances shall not be inferred—

(1) from any provision of law (whether or not in effect before November 7, 1973), including any provision contained in any appropriation Act, unless such provision specifically authorizes the introduction of United States Armed Forces into hostilities or into such situations and states that it is intended to constitute specific statutory authorization within the meaning of this chapter; or

(2) from any treaty heretofore or hereafter ratified unless such treaty is implemented by legislation specifically authorizing the introduction of United States Armed Forces into hostilities or into such situations and stating that it is intended to constitute specific statutory authorization within the meaning of this chapter.

(b) Joint headquarters operations of high-level military commands

Nothing in this chapter shall be construed to require any further specific statutory authorization to permit members of United States Armed Forces to participate jointly with members of the armed forces of one or more foreign countries in the headquarters operations of high-level military commands which were established prior to November 7, 1973, and pursuant to the United Nations Charter or any treaty ratified by the United States prior to such date.

(c) Introduction of United States Armed Forces

For purposes of this chapter, the term “introduction of United States Armed Forces” includes the assignment of members of such armed forces to command, coordinate, participate in the movement of, or accompany the regular or irregular military forces of any foreign country or government when such military forces are engaged, or there exists an imminent threat that such forces will become engaged, in hostilities.
(d) Constitutional authorities or existing treaties unaffected; construction against grant of Presidential authority respecting use of United States Armed Forces

Nothing in this chapter--

(1) is intended to alter the constitutional authority of the Congress or of the President, or the provisions of existing treaties; or

(2) shall be construed as granting any authority to the President with respect to the introduction of United States Armed Forces into hostilities or into situations wherein involvement in hostilities is clearly indicated by the circumstances which authority he would not have had in the absence of this chapter.

CREDIT(S)


HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports


Effective and Applicability Provisions


LAW REVIEW COMMENTARIES

Rethinking the role of the war powers resolution: Congress and the Persian Gulf War. Eileen Burgin, 21 J.Legis. 23 (1995).

LIBRARY REFERENCES

American Digest System

War and National Emergency 35.
Key Number System Topic No. 402.

NOTES OF DECISIONS

Central Intelligence Agency operations 2

Effective:[See Text Amendments]

United States Code Annotated Currentness
Title 50. War and National Defense (Refs & Annos)
  Chapter 33. War Powers Resolution (Refs & Annos)
    § 1548. Separability

If any provision of this chapter or the application thereof to any person or circumstance is held invalid, the remainder of the chapter and the application of such provision to any other person or circumstance shall not be affected thereby.

CREDIT(S)

HISTORICAL AND STATUTORY NOTES
Revision Notes and Legislative Reports

Effective and Applicability Provisions

LIBRARY REFERENCES
American Digest System
  Statutes C–64(1).
  Key Number System Topic No. 361.

50 U.S.C.A. § 1548, 50 USCA § 1548

Current through P.L. 113-36 approved 9-18-13

Legal Fears Slowed Aid to Syrian Rebels
By Adam Entous, Wall Street Journal, July 14, 2013

A string of cautionary opinions from administration lawyers over the last two years sheds new light on President Barrack Obama’s halting and ultimately secretive steps to provide military support to rebels in Syria's deadly civil war.

Members of the so-called Lawyers Group of top legal advisers from across the administration argued that Mr. Obama risked violating international law and giving Syrian President Bashar al-Assad the legal grounds—and motivation—to retaliate against Americans, said current and former officials.

The group's arguments in part help explain why the White House agonized over Syria intervention and why Mr. Obama eventually opted to provide military aid to the rebels covertly through the Central Intelligence Agency, to help mitigate the legal risks and keep the U.S.’s profile low.

Administration lawyers recently determined that providing such aid was allowed under U.S. domestic law, helping to clear the way for limited arms shipments to handpicked groups of rebels likely starting in August. But the lawyers sidestepped questions over international law by asserting that supporting the rebels was justified by a number of factors: the humanitarian crisis in Syria, alleged human-rights violations by the regime and Iranian arms shipments that violate U.N. Security Council sanctions.

"They are assuming the risks," said a former administration official involved in the legal debate.

Experts say President Bill Clinton took a similar approach in justifying the Kosovo bombing campaign in 1999, which, like the Syria effort, wasn't authorized by the U.N. Security Council.

"An old trial lawyer adage is that when the law is not on your side, argue the facts instead," said John Bellinger, a former State Department legal adviser during the Bush administration. "Here, the [administration] is saying that the aid is permissible under U.S. domestic law but is careful to avoid saying the aid is permissible under international law."

U.N. Security Council resolutions that could authorize outside intervention in Syria have been blocked by Russia, which was critical of the North Atlantic Treaty Organization-led mission in Libya in 2011, constraining the U.S.'s legal options.

As a consequence of the decision to provide support through the CIA, officials say, U.S. military aid to rebel forces is more limited than it would have been had it gone through the military.

The CIA's arming of the rebels is expected to begin now that a tentative accord has been reached with lawmakers who had threatened to freeze some funding, officials
said. Lawmakers are still demanding that the administration report back with further justification for the CIA program before taking additional action, officials say.

A reconstruction of the debate over arming the Syrian opposition shows how much administration lawyers played a cautionary role in the process, parrying calls for more assertive U.S. action by citing the risks of skirting international law, triggering a shooting war and setting legal precedents that could be cited by other countries, such as Russia and China.

At the State Department, lawyers reviewing the proposals found themselves at odds with their more forward-leaning bosses — former Secretary of State Hillary Clinton and now John Kerry — who both pushed a reluctant Mr. Obama to ramp up military support to the rebels, including through the provision of arms.

Some of the lawyers involved were uncomfortable with what they saw as a policy that could be seen as similar to the Reagan administration's backing of Nicaragua's Contra guerrillas in the 1980s.

Some of them cited a 1986 decision from the International Court of Justice on the American role in Nicaragua that said the U.S. was in "breach of its obligation under customary international law not to intervene in the affairs of another state."

U.S. officials give two possible explanations as to why the lawyers were cautious. Some say it reflected the extent to which Mr. Obama and his legal advisers sought to draw a distinction with the Bush administration and its approach to international law. Others say it reflected Mr. Obama's deep reluctance to take steps that could lead the U.S. into another war in the Middle East. The Lawyers Group, which has existed in previous administrations, works by consensus in order to avoid presenting "the client"—the president—with split legal decisions.

Key members of the group raised objections soon after the start of the Syrian uprising, in March 2011, when some in the State Department argued for recognizing the opposition and severing ties to the regime, said current and former officials.

Then-State Department legal adviser Harold Koh and other administration lawyers argued that could be viewed as meaning the U.S. no longer recognized Mr. Assad's government, officials involved in the debate said.

That, they argued, could relieve him of his responsibilities under international law such things as the use of chemical weapons under his government's control. After months of internal debate, the administration called on Mr. Assad to "step aside" but didn't recognize the opposition.

In summer 2012, the White House began to focus on State Department and CIA proposals to ramp up support to the rebels, from providing nonlethal military support, including body armor and night-vision goggles, to small arms, officials say.
In response, the Lawyers Group questioned whether the State Department could provide military support directly to forces fighting a war in which the U.S. wasn't formally engaged. Lawyers also told the White House that providing military aid would allow Mr. Assad under international law to declare Americans combatants, whether in military uniforms or not, and target them for taking sides in another country's civil war. The lawyers said even a State Department proposal to supply rebel fighters with food rations could give Mr. Assad legal grounds go after Americans.

"The giving of aid is the equivalent of taking sides—if you give them guns or you give them food to survive, you're still supporting them in the effort and the other side can consider you the enemy," one former Obama administration official said.

In December, Mr. Obama recognized a Western-backed opposition coalition as the "legitimate representative of the Syrian people in opposition to the Assad regime," a carefully worded statement that administration lawyers believed stopped short of full recognition.

The legal debate over providing military support to the rebels came to a head earlier this year.

In February, Secretary of State Kerry was poised to fly to Rome where officials hoped he would announce a U.S. decision to, for the first time, provide nonlethal military equipment along with halal meals and medical kits, directly to the Western-backed rebel army of Gen. Salim Idris, current and former U.S. officials said.

At the time, the administration balked at authorizing the State Department to provide military equipment: Using the State Department to do so was "legally available" under domestic law, but questionable under international law. As a result, Mr. Kerry announced only plans to provide food rations and medical kits, disappointing the opposition.

Some lawyers continued to raise objections to even the pared-down plan, arguing that Gen. Idris's Free Syrian Army should deliver the supplies only to unarmed civilians, instead of giving them to fighters, said an official briefed on the matter.

In the end, the State Department delivered the rations and medical kits based on a legal determination that such provisions didn't count as military aid because they didn't improve the fighters' ability, officials said. Moreover, the White House decided the aid couldn't be given exclusively to fighters, but should also go to nonfighters.

While the smaller CIA footprint may reduce the risk that Mr. Assad will launch attacks on U.S. personnel arming and training rebels mainly in Jordan and diplomats and aid workers in other countries such as Lebanon, current and former officials say the legal risks remain.

The lawyers told the White House that Mr. Assad was under no obligation to draw a distinction between the CIA and other branches of the U.S. government.
"Once Assad claims a right to attack American citizens, we're in a whole new game," a former official said.

—Siobhan Gorman contributed to this article.
"THE CONFLICT AGAINST AL QAEDA AND ITS AFFILIATES: HOW WILL IT END?"

Jeh Charles Johnson

General Counsel of the U.S. Department of Defense at the Oxford Union, Oxford University[1]

November 30, 2012

Thank you for inviting me. It is a privilege for me to stand here, in the same place, before the same Union, as the Prime Ministers, Presidents, and other world notables who have preceded me.

I am the General Counsel of the U.S. Defense Department. If I had to summarize my job in one sentence: it is to ensure that everything our military and our Defense Department do is consistent with U.S. and international law. This includes the prior legal review of every military operation that the Secretary of Defense and the President must approve.

My counterpart here in the United Kingdom is Ms. Frances Nash, the legal adviser to the U.K. Ministry of Defence. Like Ms. Nash, I am a civilian, not a member of the military, consistent with the principle in both our countries of civilian oversight of the military. Unlike Ms. Nash, who is a civil servant and a long-time official of the Ministry of Defence, I am a political appointee. This means I serve at the pleasure of the current President, and have no expectation of serving for any other.

Here in the United Kingdom, you refer to July 7, 2005, the day of the terrorist suicide bombings of the London subway, as “7/7.” I am a New Yorker and a personal witness to the events of “9/11.” I was a private citizen then, and like many others that day, wandered the streets of Manhattan asking: “what can I do to help?”

Over the last 46 months as a public official, I have tried to answer that question. There is a quote from the Brookings Institution in Washington, which motivates my own public service:

American government was designed to be led by citizens who would step out of private life for a term of office, then return to their communities enriched by service and ready to recruit the next generation of citizen servants. The Founding Fathers believed in a democracy led by individuals who would not become so enamored of power and addicted to perquisites that they use government as an instrument of self-aggrandizement.

Indeed, it was the British poet Lord Byron who called our First President, George Washington, the “Cincinnatus of the West” for his decision to surrender his personal power after the American Revolution and retire to his farm on Mount Vernon.21
As a member of the Obama Administration for the last four years, I have been privileged to witness many transformational and historic events in the national security of the United States.

We ended the combat mission in Iraq.

We increased the number of combat forces in Afghanistan and have reversed much of the Taliban’s momentum in the country. Challenges remain, but violence is down across the country. We have a timetable for transitioning our efforts in Afghanistan to the Afghans’ own security forces, and we are adhering to it. And though we have disagreed with our Afghan partners from time to time, as of this date we have negotiated and signed understandings with the Afghan government on detention operations,[3] special operations[4] and an overall strategic partnership.[5] representing major milestones toward the day when the peace and security of that country is fully in the hands of the Afghan people and their government.

I was in Afghanistan last week, to spend Thanksgiving with the troops. While there I encountered a number of Her Majesty’s armed forces. The British subjects here should be proud of them all. The British hospital I visited at Camp Bastion was first-rate and amazing. And the very good news on that particular day was, at three separate hospitals, I saw not a single U.S. or UK casualty, except for a U.S. soldier in need of an appendectomy, a British soldier with a bad knee, and many bored and happy trauma teams standing around with nothing to do.

We banned “enhanced interrogation techniques,” consistent with the calls of many in our country, including our own military, that great nations simply do not treat other human beings that way. These controversial practices have been banned, yet we continue to gather valuable intelligence in a manner consistent with our Army Field Manual, the Detainee Treatment Act, and international law.

We worked with our Congress to enact the Military Commissions Act of 2009, which reformed our system of military commissions to ensure due process and fairness for the accused. Today, our system of military commissions prosecutions of Khalid Sheik Mohammed and the other alleged organizers of the September 11 attacks is more credible, sustainable and transparent. One of our nation’s finest military lawyers, and a Rhodes Scholar, Brigadier General Mark Martins, is now the chief prosecutor in that system.

We worked with our Congress to pass the Don’t Ask, Don’t Tell Repeal Act of 2010, such that gay and lesbian members of the U.S. military can now be open and honest about their sexual orientation without fear of being separated for that reason. In
the words of one gay servicemember: “you took a knife out of my back; you have no idea what it is like to serve in silence.”

And, finally, we have, in a manner consistent with our laws and values, taken the fight directly to the terrorist organization al Qaeda, the result of which is that the core of al Qaeda is today degraded, disorganized and on the run. Osama bin Laden is dead. Many other leaders and terrorist operatives of al Qaeda are dead or captured; those left in al Qaeda’s core struggle to communicate, issue orders, and recruit.

But, there is still danger and there is still much to do. Al Qaeda’s core has been degraded, leaving al Qaeda more decentralized, and most terrorist activity now conducted by local franchises, such as Al Qaeda in the Arabian Peninsula (based in Yemen) and Al Qaeda in the Islamic Maghreb (operating in north and west Africa). So, therefore, in places like Yemen, and in partnership with that government, we are taking the fight directly to AQAP, and continually disrupting its plans to conduct terrorist attacks against U.S. and Yemeni interests.

Al Qaeda has sought to attack the UK on a number of occasions. Two years ago, Her Majesty’s government assessed:

“We face a real and pressing threat from international terrorism, particularly that inspired by Al Qaeda and its affiliates . . . Al Qaeda remains the most potent terrorist threat to the UK.”[6]

Our efforts against al Qaeda have involved multiple instruments of the U.S. government, including the military, civilian law enforcement, and intelligence services, in partnership with the United Kingdom and other nations.

It is the U.S. military’s efforts against al Qaeda and associated forces that has demanded most of my time, generated much public legal commentary, and presented for us what are perhaps the weightiest legal issues in national security. It is the topic I will spend the balance of my remarks on tonight.

The United States government is in an armed conflict against al Qaeda and associated forces, to which the laws of armed conflict apply. One week after 9/11, our Congress authorized our President to “to use all necessary and appropriate force” against those nations, organizations and individuals responsible for 9/11. President Obama, like President Bush before him, as Commander-in-Chief of our Armed Forces, has acted militarily based on that authorization. In 2006, our Supreme Court also endorsed the view that the United States is in an armed conflict with al Qaeda.[7] Therefore, all three branches of the United States government – including the two political branches elected by the people and the judicial branch appointed for life (and therefore not subject to the
whims and political pressures of the voters) – have endorsed the view that our efforts against al Qaeda may properly be viewed as an armed conflict.

But, for the United States, this is a new kind of war. It is an unconventional war against an unconventional enemy. And, given its unconventional nature, President Obama – himself a lawyer and a good one – has insisted that our efforts in pursuit of this enemy stay firmly rooted in conventional legal principles. For, in our efforts to destroy and dismantle al Qaeda, we cannot dismantle our laws and our values, too.

The danger of al Qaeda is well known. It is a terrorist organization determined to commit acts of violence against innocent civilians. The danger of the conflict against al Qaeda is that it lacks conventional boundaries, against an enemy that does not observe the rules of armed conflict, does not wear a uniform, and can resemble a civilian.

But we refuse to allow this enemy, with its contemptible tactics, to define the way in which we wage war. Our efforts remain grounded in the rule of law. In this unconventional conflict, therefore, we apply conventional legal principles – conventional legal principles found in treaties and customary international law.

As in armed conflict, we have been clear in defining the enemy and defining our objective against that enemy.

We have made clear that we are not at war with an idea, a religion, or a tactic. We are at war with an organized, armed group — a group determined to kill innocent civilians.

We have publicly stated that our enemy consists of those persons who are part of the Taliban, al-Qaeda or associated forces, a declaration that has been embraced by two U.S. Presidents, accepted by our courts, and affirmed by our Congress.

We have publicly defined an “associated force” as having two characteristics: (1) an organized, armed group that has entered the fight alongside al Qaeda, and (2) is a co-belligerent with al Qaeda in hostilities against the United States or its coalition partners.

Our enemy does not include anyone solely in the category of activist, journalist, or propagandist.

Nor does our enemy in this armed conflict include a “lone wolf” who, inspired by al Qaeda’s ideology, self-radicalizes in the basement of his own home, without ever actually becoming part of al Qaeda. Such persons are dangerous, but are a matter for civilian law enforcement, not the military, because they are not part of the enemy force.

And, we have publicly stated that our goal in this conflict is to “disrupt, dismantle, and ensure a lasting defeat of al Qaeda and violent extremist affiliates.”
Some legal scholars and commentators in our country brand the detention by the military of members of al Qaeda as "indefinite detention without charges." Some refer to targeted lethal force against known, identified individual members of al Qaeda as "extrajudicial killing."

Viewed within the context of law enforcement or criminal justice, where no person is sentenced to death or prison without an indictment, an arraignment, and a trial before an impartial judge or jury, these characterizations might be understandable.

Viewed within the context of conventional armed conflict — as they should be — capture, detention and lethal force are traditional practices as old as armies. Capture and detention by the military are part and parcel of armed conflict.[13] We employ weapons of war against al Qaeda, but in a manner consistent with the law of war. We employ lethal force, but in a manner consistent with the law of war principles of proportionality, necessity and distinction. We detain those who are part of al Qaeda, but in a manner consistent with Common Article 3 of the Geneva Conventions and all other applicable law.[14]

But, now that efforts by the U.S. military against al Qaeda are in their 12th year, we must also ask ourselves: how will this conflict end? It is an unconventional conflict, against an unconventional enemy, and will not end in conventional terms.

Conventional conflicts in history tend to have had conventional endings.

Two hundred years ago, our two Nations fought the War of 1812. The United States lost many battles, Washington, DC was captured, and the White House was set ablaze. By the winter of 1814 British and American forces had strengthened their forts and fleets, and assumed that fighting would resume between them in the spring. But, the war ended when British and American diplomats in Belgium came to a peace agreement on December 24, 1814. Diplomats from both sides then joined together in a Christmas celebration at Ghent cathedral. Less than eight weeks later, the U.S. Senate provided advice and consent to that peace treaty, which for the United States legally and formally terminated the conflict.[15]

In the American Civil War, the Battle of Appomattox was the final engagement of Confederate General Robert E. Lee’s great Army of Northern Virginia, and one of the last battles of that war. After four years of war, General Lee recognized that “[i]t would be useless and therefore cruel to provoke the further effusion of blood.” Three days later the Army of Northern Virginia surrendered.[16] Lee’s army then marched to the field in front of Appomattox Court House, and, division by division, deployed into line, stacked their arms, folded their colors, and walked home empty-handed.[17]
The last day of the First World War was November 11, 1918, when an armistice was signed at 5:00 a.m. in a railroad carriage in France, and a ceasefire took effect on the eleventh hour of the eleventh day of the eleventh month of 1918.

The Second World War concluded in the Pacific theater in August 1945, with a ceremony that took place on the deck of the USS Missouri.

During the Gulf War of 1991, one week after Saddam Hussein’s forces set fire to oil wells as they were driven out of Kuwait, U.S. General Schwarzkopf sat down with Iraqi military leaders under a tent in a stretch of the occupied Iraqi desert a few miles from the Kuwaiti border. General Schwarzkopf wanted to keep discussions simple; he told his advisors: “I just want to get my soldiers home as fast as possible . . . I want no ceremonies, no handshakes.”[18] In the space of two hours they had negotiated the terms of a permanent cease-fire to end the First Gulf War.[19]

We cannot and should not expect al Qaeda and its associated forces to all surrender, all lay down their weapons in an open field, or to sign a peace treaty with us. They are terrorist organizations. Nor can we capture or kill every last terrorist who claims an affiliation with al Qaeda.

I am aware of studies that suggest that many “terrorist” organizations eventually denounce terrorism and violence, and seek to address their grievances through some form of reconciliation or participation in a political process.[20]

Al Qaeda is not in that category.

Al Qaeda’s radical and absurd goals have included global domination through a violent Islamic caliphate, terrorizing the United States and other western nations from retreating from the world stage,[21] and the destruction of Israel. There is no compromise or political bargain that can be struck with those who pursue such aims.

In the current conflict with al Qaeda, I can offer no prediction about when this conflict will end, or whether we are, as Winston Churchill described it, near the “beginning of the end.”

I do believe that on the present course, there will come a tipping point – a tipping point at which so many of the leaders and operatives of al Qaeda and its affiliates have been killed or captured, and the group is no longer able to attempt or launch a strategic attack against the United States, such that al Qaeda as we know it, the organization that our Congress authorized the military to pursue in 2001, has been effectively destroyed.
At that point, we must be able to say to ourselves that our efforts should no longer be considered an “armed conflict” against al Qaeda and its associated forces; rather, a counterterrorism effort against individuals who are the scattered remnants of al Qaeda, or are parts of groups unaffiliated with al Qaeda, for which the law enforcement and intelligence resources of our government are principally responsible, in cooperation with the international community – with our military assets available in reserve to address continuing and imminent terrorist threats.

At that point we will also need to face the question of what to do with any members of al Qaeda who still remain in U.S. military detention without a criminal conviction and sentence. In general, the military’s authority to detain ends with the “cessation of active hostilities.”[22] For this particular conflict, all I can say today is that we should look to conventional legal principles to supply the answer, and that both our Nations faced similar challenging questions after the cessation of hostilities in World War II, and our governments delayed the release of some Nazi German prisoners of war.[23]

For now, we must continue our efforts to disrupt, dismantle and ensure a lasting defeat of al Qaeda. Though severely degraded, al Qaeda remains a threat to the citizens of the United States, the United Kingdom and other nations. We must disrupt al Qaeda’s terrorist attack planning before it gets anywhere near our homeland or our citizens. We must counter al Qaeda in the places where it seeks to establish safe haven, and prevent it from reconstituting in others. To do this we must utilize every national security element of our government, and work closely with our friends and allies like the United Kingdom and others.

Finally, it was a warfighting four-star general who reminded me, as I previewed these remarks for him, that none of this will ever be possible if we fail to understand and address what attracts a young man to an organization like al Qaeda in the first place. Al Qaeda claims to represent the interests of all Muslims. By word and deed, we must stand with the millions of people within the Muslim world who reject Al Qaeda as a marginalized, extreme and violent organization that does not represent the Muslim values of peace and brotherhood. For, if al Qaeda can recruit new terrorists to its cause faster than we can kill or capture them, we fight an endless, hopeless battle that only perpetuates a downward spiral of hate, recrimination, violence and fear.

“War” must be regarded as a finite, extraordinary and unnatural state of affairs. War permits one man – if he is a “privileged belligerent,” consistent with the laws of war — to kill another. War violates the natural order of things, in which children bury their parents; in war parents bury their children. In its 12th year, we must not accept the
current conflict, and all that it entails, as the “new normal.” Peace must be regarded as the norm toward which the human race continually strives.

Right here at Oxford you have the excellent work of the Changing Character of War program: leading scholars committed to the study of war, who have observed that analyzing war in terms of a continuum of armed conflict — where military force is used at various points without a distinct break between war and peace — is counterproductive. Such an approach, they argue, results in an erosion of “any demarcation between war and peace,” the very effect of which is to create uncertainty about how to define war itself.[24]

I did not go to Oxford. I am a graduate of a small, all-male historically black college in the southern part of the United States, Morehouse College. The guiding light for every Morehouse man is our most famous alumnus, Martin Luther King, who preached the inherent insanity of all wars. I am therefore a student and disciple of Dr. King — though I became an imperfect one the first time I gave legal approval for the use of military force. I accepted this conundrum when I took this job. But, I still carry with me the words from Dr. King: “Returning hate for hate multiplies hate, adding deeper darkness to a night already devoid of stars … violence multiplies violence, and toughness multiplies toughness in a descending spiral of destruction … The chain reaction of evil—hate begetting hate, wars producing more wars—must be broken, or we shall be plunged into the dark abyss of annihilation.”[25]

Thank you again for the honor and the opportunity to be in this special place, and thank you for listening to me.

[1] With the valuable research assistance of David A. Simon, Special Counsel to the General Counsel (J.D., Harvard Law School; M.Phil., International Relations, Oxford University).
[17] Id. at 630-631


[23] Regarding post-hostilities detention during the conclusion of World War II, see Ludecke v. Watkins 335 U.S. 160 (1948) (holding that the President’s authority to detain German nationals continued for over six years after the fighting with Germany had ended); See also Alien Enemy Act of 1798 50 U.S.C. §§21-24 (2000). See James Richards, British Broadcasting Corporation, Life in Britain for German Prisoners of War, (noting that by the end of 1947, 250,000 of the prisoners of war were repatriated, and the last repatriation took place in November 1948), available at: http://www.bbc.co.uk/history/british/britain_wwtwo/german_pows_01.shtml.


AFGHAN WAR’S APPROACHING END THROWS LEGAL STATUS OF GUANTANAMO DETAINEES INTO DOUBT

By Karen DeYoung, Washington Post October 18, 2013

The approaching end of the U.S. war in Afghanistan could help President Obama move toward what he has said he wanted to do since his first day in office: close the U.S. prison at Guantanamo Bay, Cuba.

Blocked by Congress from releasing or transferring many of the remaining 164 detainees and able to try only a small number of them, administration officials are examining whether the withdrawal of U.S. troops at the end of 2014 could open the door for some to challenge the legal authority of the United States to continue to imprison them.

Most immediately, officials believe the war’s declared end could force a reckoning over the detention of more than a dozen Afghan Taliban members captured on the battlefield, allowing them to lodge new appeals to the federal courts.

“In the words of the Supreme Court, the authority to detain — if you’re detaining based on someone being a belligerent — can unravel as hot wars end. And I think that’s a real question,” Brig. Gen. Mark Martins, chief prosecutor for military commissions at Guantanamo, said in a recent interview.

Detainees at Guantanamo have been held, some of them for more than 12 years and most without charge, since Congress authorized the use of military force against those who “planned, authorized, committed or aided” the Sept. 11, 2001, attacks and might launch new attacks.

Ideally, Obama would like to do away with the Authorization for the Use of Military Force, a law passed within days of the 9/11 attacks, and replace it with more targeted versions to allow action against new al-Qaeda related groups in the Middle East and Africa and other threats as they arise. His goal, the president said in a May Speech, is to ”refine, and ultimately repeal” the existing authority.

Repeal of the AUMF could allow other detainees imprisoned under its terms to refile habeas corpus petitions that the government had successfully quashed.

“If that were to go away, you really don’t have that legal hook for continued detention,” a senior administration official said of the AUMF. “I think you would have some very interesting constitutional questions.”

While the end of the war may accelerate the transfer of prisoners, the administration would still need a place to hold those being tried in military commissions,
including the alleged 9/11 plotters, and potentially some of the four dozen men deemed too dangerous to release but who are ineligible for trial because evidence against them is inadmissible. Congress has prohibited their transfer to U.S. prisons.

No new detainees have arrived at Guantanamo since 2008, when the George W. Bush administration announced the transfer of the last of the 16 “high-value” prisoners from secret CIA and other sites overseas.

Under both the Bush and Obama administrations, the AUMF has provided the legal justification under U.S. law for military action in Afghanistan and for CIA drone attacks and other actions in Pakistan. With no legislative or legal challenge, Obama has also adopted a more expanded interpretation of the law to use force against al-Qaeda “associates,” including groups that did not exist when it was first enacted.

As currently interpreted, the AUMF has no geographic boundaries and can justify military action anywhere in the world where the administration determines it applies. Under Obama, it has been the legal underpinning for lethal strikes against Yemen-based al-Qaeda in the Arabian Peninsula and al-Shabab in Somalia. Earlier this month, it was the cited legal authority for U.S. Special Forces operations that captured Nazih Abdul-Hamed al-Ruqai, also known as Anas al-Libi, in Tripoli, Libya, and the failed attempt to capture an al-Shabab leader in southern Somalia.

But the open-ended nature of the AUMF — along with the distance in time and space between current struggles in the Middle East and Africa and the Afghan conflict that began in 2001 — has left many concerned.

“I never imagined that the AUMF would still be in effect today,” former Rep. Jane Harman (D-Calif.), one of 420 House members to vote in favor of the measure on Sept. 14, 2001, said at a recent conference on the subject.

“Over time, some would assert, and I agree, that it has taken on a life of its own, and the executive branch has used it in ways that no one who voted for it envisioned,” Harman said.

Others have been reluctant to do away with it or narrow its scope, in part because of the potential effect its demise could have on Guantanamo.

The only ironclad waiver to the current congressional restrictions on transferring detainees out of Guantanamo Bay is a court order. “All the folks who remain there have lost — or, depending on your perspective, the government has won -- habeas [corpus] litigation,” said the senior official, who spoke on the condition of anonymity to discuss internal administration deliberations.
“If that goes away,” the official said, a raft of new petitions is expected, along with new pressure on Congress to lift three-year-old restrictions on transfers home or to other countries.

Thus far, the administration has made no move to implement Obama’s goal of narrowing or doing away with the AUMF. An amendment proposed last summer by Rep. Adam Schiff (D-Calif.) to end the authority after the last U.S. combat troops leave Afghanistan in December 2014 was defeated 236 to 180.

Ending the AUMF “forces the issue,” Schiff said in an interview. “It doesn’t mean there would have to be some precipitous decision” on Guantanamo, he said, noting that prisoners of past wars have sometimes been held long after fighting ended. “But the clock would very much be ticking.”

Jeh Johnson, the former general counsel for the Defense Department who has just been nominated to head the Department of Homeland Security, noted in a 2012 speech that the release of some German prisoners of war was delayed for years after the end of World War II, which a 1948 Supreme Court case found was within the executive powers of the president.

But “in general,” Johnson said, “the military’s authority to detain ends with the cessation of active hostilities.” Billy Kenber contributed to this report.
THE WHITE HOUSE
Office of the Press Secretary

May 23, 2013

The Future of our Fight against Terrorism
Remarks of President Barack Obama – As Prepared for Delivery
National Defense University
May 23, 2013

As Prepared for Delivery –

It’s an honor to return to the National Defense University. Here, at Fort McNair, Americans have served in uniform since 1791– standing guard in the early days of the Republic, and contemplating the future of warfare here in the 21st century.

For over two centuries, the United States has been bound together by founding documents that defined who we are as Americans, and served as our compass through every type of change. Matters of war and peace are no different. Americans are deeply ambivalent about war, but having fought for our independence, we know that a price must be paid for freedom. From the Civil War, to our struggle against fascism, and through the long, twilight struggle of the Cold War, battlefields have changed, and technology has evolved. But our commitment to Constitutional principles has weathered every war, and every war has come to an end.

With the collapse of the Berlin Wall, a new dawn of democracy took hold abroad, and a decade of peace and prosperity arrived at home. For a moment, it seemed the 21st century would be a tranquil time. Then, on September 11th 2001, we were shaken out of complacency. Thousands were taken from us, as clouds of fire, metal and ash descended upon a sun-filled morning. This was a different kind of war. No armies came to our shores, and our military was not the principal target. Instead, a group of terrorists came to kill as many civilians as they could.

And so our nation went to war. We have now been at war for well over a decade. I won’t review the full history. What’s clear is that we quickly drove al Qaeda out of Afghanistan, but then shifted our focus and began a new war in Iraq. This carried grave consequences for our fight against al Qaeda, our standing in the world, and – to this day – our interests in a vital region.

Meanwhile, we strengthened our defenses – hardening targets, tightening transportation security, and giving law enforcement new tools to prevent terror. Most of these changes were sound. Some caused inconvenience. But some, like expanded surveillance, raised difficult questions about the balance we strike between our interests in security and our values of privacy. And in some cases, I believe we compromised our
basic values – by using torture to interrogate our enemies, and detaining individuals in
a way that ran counter to the rule of law.

After I took office, we stepped up the war against al Qaeda, but also sought to change
its course. We relentlessly targeted al Qaeda’s leadership. We ended the war in Iraq,
and brought nearly 150,000 troops home. We pursued a new strategy in Afghanistan,
and increased our training of Afghan forces. We unequivocally banned torture,
affirmed our commitment to civilian courts, worked to align our policies with the rule
of law, and expanded our consultations with Congress.

Today, Osama bin Laden is dead, and so are most of his top lieutenants. There have
been no large-scale attacks on the United States, and our homeland is more secure.
Fewer of our troops are in harm’s way, and over the next 19 months they will continue
to come home. Our alliances are strong, and so is our standing in the world. In sum, we
are safer because of our efforts.

Now make no mistake: our nation is still threatened by terrorists. From Benghazi to
Boston, we have been tragically reminded of that truth. We must recognize, however,
that the threat has shifted and evolved from the one that came to our shores on 9/11.
With a decade of experience to draw from, now is the time to ask ourselves hard
questions – about the nature of today’s threats, and how we should confront them.

These questions matter to every American. For over the last decade, our nation has
spent well over a trillion dollars on war, exploding our deficits and constraining our
ability to nation build here at home. Our service-members and their families have
sacrificed far more on our behalf. Nearly 7,000 Americans have made the ultimate
sacrifice. Many more have left a part of themselves on the battlefield, or brought the
shadows of battle back home. From our use of drones to the detention of terrorist
suspects, the decisions we are making will define the type of nation – and world – that
we leave to our children.

So America is at a crossroads. We must define the nature and scope of this struggle, or
else it will define us, mindful of James Madison’s warning that “No nation could
preserve its freedom in the midst of continual warfare.” Neither I, nor any President,
can promise the total defeat of terror. We will never erase the evil that lies in the hearts
of some human beings, nor stamp out every danger to our open society. What we can
do – what we must do – is dismantle networks that pose a direct danger, and make it
less likely for new groups to gain a foothold, all while maintaining the freedoms and
ideals that we defend. To define that strategy, we must make decisions based not on
fear, but hard-earned wisdom. And that begins with understanding the threat we face.

Today, the core of al Qaeda in Afghanistan and Pakistan is on a path to defeat. Their
remaining operatives spend more time thinking about their own safety than plotting
against us. They did not direct the attacks in Benghazi or Boston. They have not carried
out a successful attack on our homeland since 9/11. Instead, what we’ve seen is the
emergence of various al Qaeda affiliates. From Yemen to Iraq, from Somalia to North Africa, the threat today is more diffuse, with Al Qaeda’s affiliate in the Arabian Peninsula – AQAP – the most active in plotting against our homeland. While none of AQAP’s efforts approach the scale of 9/11 they have continued to plot acts of terror, like the attempt to blow up an airplane on Christmas Day in 2009.

Unrest in the Arab World has also allowed extremists to gain a foothold in countries like Libya and Syria. Here, too, there are differences from 9/11. In some cases, we confront state-sponsored networks like Hezbollah that engage in acts of terror to achieve political goals. Others are simply collections of local militias or extremists interested in seizing territory. While we are vigilant for signs that these groups may pose a transnational threat, most are focused on operating in the countries and regions where they are based. That means we will face more localized threats like those we saw in Benghazi, or at the BP oil facility in Algeria, in which local operatives – in loose affiliation with regional networks – launch periodic attacks against Western diplomats, companies, and other soft targets, or resort to kidnapping and other criminal enterprises to fund their operations.

Finally, we face a real threat from radicalized individuals here in the United States. Whether it’s a shooter at a Sikh Temple in Wisconsin; a plane flying into a building in Texas; or the extremists who killed 168 people at the Federal Building in Oklahoma City – America has confronted many forms of violent extremism in our time. Deranged or alienated individuals – often U.S. citizens or legal residents – can do enormous damage, particularly when inspired by larger notions of violent jihad. That pull towards extremism appears to have led to the shooting at Fort Hood, and the bombing of the Boston Marathon.

Lethal yet less capable al Qaeda affiliates. Threats to diplomatic facilities and businesses abroad. Homegrown extremists. This is the future of terrorism. We must take these threats seriously, and do all that we can to confront them. But as we shape our response, we have to recognize that the scale of this threat closely resembles the types of attacks we faced before 9/11. In the 1980s, we lost Americans to terrorism at our Embassy in Beirut; at our Marine Barracks in Lebanon; on a cruise ship at sea; at a disco in Berlin; and on Pan Am Flight 103 over Lockerbie. In the 1990s, we lost Americans to terrorism at the World Trade Center; at our military facilities in Saudi Arabia; and at our Embassy in Kenya. These attacks were all deadly, and we learned that left unchecked, these threats can grow. But if dealt with smartly and proportionally, these threats need not rise to the level that we saw on the eve of 9/11.

Moreover, we must recognize that these threats don’t arise in a vacuum. Most, though not all, of the terrorism we face is fueled by a common ideology – a belief by some extremists that Islam is in conflict with the United States and the West, and that violence against Western targets, including civilians, is justified in pursuit of a larger cause. Of course, this ideology is based on a lie, for the United States is not at war with
Islam; and this ideology is rejected by the vast majority of Muslims, who are the most frequent victims of terrorist acts.

Nevertheless, this ideology persists, and in an age in which ideas and images can travel the globe in an instant, our response to terrorism cannot depend on military or law enforcement alone. We need all elements of national power to win a battle of wills and ideas. So let me discuss the components of such a comprehensive counter-terrorism strategy.

First, we must finish the work of defeating al Qaeda and its associated forces.

In Afghanistan, we will complete our transition to Afghan responsibility for security. Our troops will come home. Our combat mission will come to an end. And we will work with the Afghan government to train security forces, and sustain a counter-terrorism force which ensures that al Qaeda can never again establish a safe-haven to launch attacks against us or our allies.

Beyond Afghanistan, we must define our effort not as a boundless 'global war on terror' - but rather as a series of persistent, targeted efforts to dismantle specific networks of violent extremists that threaten America. In many cases, this will involve partnerships with other countries. Thousands of Pakistani soldiers have lost their lives fighting extremists. In Yemen, we are supporting security forces that have reclaimed territory from AQAP. In Somalia, we helped a coalition of African nations push al Shabaab out of its strongholds. In Mali, we are providing military aid to a French-led intervention to push back al Qaeda in the Maghreb, and help the people of Mali reclaim their future.

Much of our best counter-terrorism cooperation results in the gathering and sharing of intelligence; the arrest and prosecution of terrorists. That's how a Somali terrorist apprehended off the coast of Yemen is now in prison in New York. That's how we worked with European allies to disrupt plots from Denmark to Germany to the United Kingdom. That's how intelligence collected with Saudi Arabia helped us stop a cargo plane from being blown up over the Atlantic.

But despite our strong preference for the detention and prosecution of terrorists, sometimes this approach is foreclosed. Al Qaeda and its affiliates try to gain a foothold in some of the most distant and unforgiving places on Earth. They take refuge in remote tribal regions. They hide in caves and walled compounds. They train in empty deserts and rugged mountains.

In some of these places - such as parts of Somalia and Yemen - the state has only the most tenuous reach into the territory. In other cases, the state lacks the capacity or will to take action. It is also not possible for America to simply deploy a team of Special Forces to capture every terrorist. And even when such an approach may be possible, there are places where it would pose profound risks to our troops and local civilians - where a terrorist compound cannot be breached without triggering a firefight with
surrounding tribal communities that pose no threat to us, or when putting U.S. boots on the ground may trigger a major international crisis.

To put it another way, our operation in Pakistan against Osama bin Laden cannot be the norm. The risks in that case were immense; the likelihood of capture, although our preference, was remote given the certainty of resistance; the fact that we did not find ourselves confronted with civilian casualties, or embroiled in an extended firefight, was a testament to the meticulous planning and professionalism of our Special Forces – but also depended on some luck. And even then, the cost to our relationship with Pakistan – and the backlash among the Pakistani public over encroachment on their territory – was so severe that we are just now beginning to rebuild this important partnership.

It is in this context that the United States has taken lethal, targeted action against al Qaeda and its associated forces, including with remotely piloted aircraft commonly referred to as drones. As was true in previous armed conflicts, this new technology raises profound questions about who is targeted, and why; about civilian casualties, and the risk of creating new enemies; about the legality of such strikes under U.S. and international law; about accountability and morality.

Let me address these questions. To begin with, our actions are effective. Don’t take my word for it. In the intelligence gathered at bin Laden’s compound, we found that he wrote, “we could lose the reserves to the enemy’s air strikes. We cannot fight air strikes with explosives.” Other communications from al Qaeda operatives confirm this as well. Dozens of highly skilled al Qaeda commanders, trainers, bomb makers, and operatives have been taken off the battlefield. Plots have been disrupted that would have targeted international aviation, U.S. transit systems, European cities and our troops in Afghanistan. Simply put, these strikes have saved lives.

Moreover, America’s actions are legal. We were attacked on 9/11. Within a week, Congress overwhelmingly authorized the use of force. Under domestic law, and international law, the United States is at war with al Qaeda, the Taliban, and their associated forces. We are at war with an organization that right now would kill as many Americans as they could if we did not stop them first. So this is a just war – a war waged proportionally, in last resort, and in self-defense.

And yet as our fight enters a new phase, America’s legitimate claim of self-defense cannot be the end of the discussion. To say a military tactic is legal, or even effective, is not to say it is wise or moral in every instance. For the same human progress that gives us the technology to strike half a world away also demands the discipline to constrain that power – or risk abusing it. That’s why, over the last four years, my Administration has worked vigorously to establish a framework that governs our use of force against terrorists – insisting upon clear guidelines, oversight and accountability that is now codified in Presidential Policy Guidance that I signed yesterday.
In the Afghan war theater, we must support our troops until the transition is complete at the end of 2014. That means we will continue to take strikes against high value al Qaeda targets, but also against forces that are massing to support attacks on coalition forces. However, by the end of 2014, we will no longer have the same need for force protection, and the progress we have made against core al Qaeda will reduce the need for unmanned strikes.

Beyond the Afghan theater, we only target al Qaeda and its associated forces. Even then, the use of drones is heavily constrained. America does not take strikes when we have the ability to capture individual terrorists - our preference is always to detain, interrogate, and prosecute them. America cannot take strikes wherever we choose - our actions are bound by consultations with partners, and respect for state sovereignty. America does not take strikes to punish individuals – we act against terrorists who pose a continuing and imminent threat to the American people, and when there are no other governments capable of effectively addressing the threat. And before any strike is taken, there must be near-certainty that no civilians will be killed or injured – the highest standard we can set.

This last point is critical, because much of the criticism about drone strikes – at home and abroad – understandably centers on reports of civilian casualties. There is a wide gap between U.S. assessments of such casualties, and non-governmental reports. Nevertheless, it is a hard fact that U.S. strikes have resulted in civilian casualties, a risk that exists in all wars. For the families of those civilians, no words or legal construct can justify their loss. For me, and those in my chain of command, these deaths will haunt us as long as we live, just as we are haunted by the civilian casualties that have occurred through conventional fighting in Afghanistan and Iraq.

But as Commander-in-Chief, I must weigh these heartbreaking tragedies against the alternatives. To do nothing in the face of terrorist networks would invite far more civilian casualties - not just in our cities at home and facilities abroad, but also in the very places - like Sana’a and Kabul and Mogadishu – where terrorists seek a foothold. Let us remember that the terrorists we are after target civilians, and the death toll from their acts of terrorism against Muslims dwarfs any estimate of civilian casualties from drone strikes.

Where foreign governments cannot or will not effectively stop terrorism in their territory, the primary alternative to targeted, lethal action is the use of conventional military options. As I’ve said, even small Special Operations carry enormous risks. Conventional firepower or missiles are far less precise than drones, and likely to cause more civilian casualties and local outrage. And invasions of these territories lead us to be viewed as occupying armies; unleash a torrent of unintended consequences; are difficult to contain; and ultimately empower those who thrive on violent conflict. So it is false to assert that putting boots on the ground is less likely to result in civilian deaths, or to create enemies in the Muslim world. The result would be more U.S. deaths, more
Blackhawks down, more confrontations with local populations, and an inevitable mission creep in support of such raids that could easily escalate into new wars.

So yes, the conflict with al Qaeda, like all armed conflict, invites tragedy. But by narrowly targeting our action against those who want to kill us, and not the people they hide among, we are choosing the course of action least likely to result in the loss of innocent life. Indeed, our efforts must also be measured against the history of putting American troops in distant lands among hostile populations. In Vietnam, hundreds of thousands of civilians died in a war where the boundaries of battle were blurred. In Iraq and Afghanistan, despite the courage and discipline of our troops, thousands of civilians have been killed. So neither conventional military action, nor waiting for attacks to occur, offers moral safe-harbor. Neither does a sole reliance on law enforcement in territories that have no functioning police or security services – and indeed, have no functioning law.

This is not to say that the risks are not real. Any U.S. military action in foreign lands risks creating more enemies, and impacts public opinion overseas. Our laws constrain the power of the President, even during wartime, and I have taken an oath to defend the Constitution of the United States. The very precision of drones strikes, and the necessary secrecy involved in such actions can end up shielding our government from the public scrutiny that a troop deployment invites. It can also lead a President and his team to view drone strikes as a cure-all for terrorism.

For this reason, I’ve insisted on strong oversight of all lethal action. After I took office, my Administration began briefing all strikes outside of Iraq and Afghanistan to the appropriate committees of Congress. Let me repeat that – not only did Congress authorize the use of force, it is briefed on every strike that America takes. That includes the one instance when we targeted an American citizen: Anwar Awlaki, the chief of external operations for AQAP.

This week, I authorized the declassification of this action, and the deaths of three other Americans in drone strikes, to facilitate transparency and debate on this issue, and to dismiss some of the more outlandish claims. For the record, I do not believe it would be constitutional for the government to target and kill any U.S. citizen – with a drone, or a shotgun – without due process. Nor should any President deploy armed drones over U.S. soil.

But when a U.S. citizen goes abroad to wage war against America – and is actively plotting to kill U.S. citizens; and when neither the United States, nor our partners are in a position to capture him before he carries out a plot – his citizenship should no more serve as a shield than a sniper shooting down on an innocent crowd should be protected from a swat team.

That’s who Anwar Awlaki was – he was continuously trying to kill people. He helped oversee the 2010 plot to detonate explosive devices on two U.S. bound cargo planes. He
was involved in planning to blow up an airliner in 2009. When Farouk Abdulmutallab –
the Christmas Day bomber – went to Yemen in 2009, Awlaki hosted him, approved his
suicide operation, and helped him tape a martyrdom video to be shown after the attack.
His last instructions were to blow up the airplane when it was over American soil. I
would have detained and prosecuted Awlaki if we captured him before he carried out a
plot. But we couldn’t. And as President, I would have been derelict in my duty had I
not authorized the strike that took out Awlaki.

Of course, the targeting of any Americans raises constitutional issues that are not
present in other strikes – which is why my Administration submitted information about
Awlaki to the Department of Justice months before Awlaki was killed, and briefed the
Congress before this strike as well. But the high threshold that we have set for taking
lethal action applies to all potential terrorist targets, regardless of whether or not they
are American citizens. This threshold respects the inherent dignity of every human life.
Alongside the decision to put our men and women in uniform in harm’s way, the
decision to use force against individuals or groups – even against a sworn enemy of the
United States – is the hardest thing I do as President. But these decisions must be made,
given my responsibility to protect the American people.

Going forward, I have asked my Administration to review proposals to extend
oversight of lethal actions outside of warzones that go beyond our reporting to
Congress. Each option has virtues in theory, but poses difficulties in practice. For
example, the establishment of a special court to evaluate and authorize lethal action has
the benefit of bringing a third branch of government into the process, but raises serious
constitutional issues about presidential and judicial authority. Another idea that’s been
suggested – the establishment of an independent oversight board in the executive
branch – avoids those problems, but may introduce a layer of bureaucracy into national-
security decision-making, without inspiring additional public confidence in the process.
Despite these challenges, I look forward to actively engaging Congress to explore these
– and other – options for increased oversight.

I believe, however, that the use of force must be seen as part of a larger discussion about
a comprehensive counter-terrorism strategy. Because for all the focus on the use of
force, force alone cannot make us safe. We cannot use force everywhere that a radical
ideology takes root; and in the absence of a strategy that reduces the well-spring of
extremism, a perpetual war – through drones or Special Forces or troop deployments –
will prove self-defeating, and alter our country in troubling ways.

So the next element of our strategy involves addressing the underlying grievances and
conflicts that feed extremism, from North Africa to South Asia. As we’ve learned this
past decade, this is a vast and complex undertaking. We must be humble in our
expectation that we can quickly resolve deep rooted problems like poverty and
sectarian hatred. Moreover, no two countries are alike, and some will undergo chaotic
change before things get better. But our security and values demand that we make the effort.

This means patiently supporting transitions to democracy in places like Egypt, Tunisia and Libya – because the peaceful realization of individual aspirations will serve as a rebuke to violent extremists. We must strengthen the opposition in Syria, while isolating extremist elements – because the end of a tyrant must not give way to the tyranny of terrorism. We are working to promote peace between Israelis and Palestinians – because it is right, and because such a peace could help reshape attitudes in the region. And we must help countries modernize economies, upgrade education, and encourage entrepreneurship – because American leadership has always been elevated by our ability to connect with peoples’ hopes, and not simply their fears.

Success on these fronts requires sustained engagement, but it will also require resources. I know that foreign aid is one of the least popular expenditures – even though it amounts to less than one percent of the federal budget. But foreign assistance cannot be viewed as charity. It is fundamental to our national security, and any sensible long-term strategy to battle extremism. Moreover, foreign assistance is a tiny fraction of what we spend fighting wars that our assistance might ultimately prevent. For what we spent in a month in Iraq at the height of the war, we could be training security forces in Libya, maintaining peace agreements between Israel and its neighbors, feeding the hungry in Yemen, building schools in Pakistan, and creating reservoirs of goodwill that marginalize extremists.

America cannot carry out this work if we do not have diplomats serving in dangerous places. Over the past decade, we have strengthened security at our Embassies, and I am implementing every recommendation of the Accountability Review Board which found unacceptable failures in Benghazi. I have called on Congress to fully fund these efforts to bolster security, harden facilities, improve intelligence, and facilitate a quicker response time from our military if a crisis emerges.

But even after we take these steps, some irreducible risks to our diplomats will remain. This is the price of being the world’s most powerful nation, particularly as a wave of change washes over the Arab World. And in balancing the trade-offs between security and active diplomacy, I firmly believe that any retreat from challenging regions will only increase the dangers we face in the long run.

Targeted action against terrorists. Effective partnerships. Diplomatic engagement and assistance. Through such a comprehensive strategy we can significantly reduce the chances of large scale attacks on the homeland and mitigate threats to Americans overseas. As we guard against dangers from abroad, however, we cannot neglect the daunting challenge of terrorism from within our borders.

As I said earlier, this threat is not new. But technology and the Internet increase its frequency and lethality. Today, a person can consume hateful propaganda, commit
themselves to a violent agenda, and learn how to kill without leaving their home. To address this threat, two years ago my Administration did a comprehensive review, and engaged with law enforcement. The best way to prevent violent extremism is to work with the Muslim American community – which has consistently rejected terrorism – to identify signs of radicalization, and partner with law enforcement when an individual is drifting towards violence. And these partnerships can only work when we recognize that Muslims are a fundamental part of the American family. Indeed, the success of American Muslims, and our determination to guard against any encroachments on their civil liberties, is the ultimate rebuke to those who say we are at war with Islam.

Indeed, thwarting homegrown plots presents particular challenges in part because of our proud commitment to civil liberties for all who call America home. That’s why, in the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are. That means reviewing the authorities of law enforcement, so we can intercept new types of communication, and build in privacy protections to prevent abuse. That means that – even after Boston – we do not deport someone or throw someone in prison in the absence of evidence. That means putting careful constraints on the tools the government uses to protect sensitive information, such as the State Secrets doctrine. And that means finally having a strong Privacy and Civil Liberties Board to review those issues where our counter-terrorism efforts and our values may come into tension.

The Justice Department’s investigation of national security leaks offers a recent example of the challenges involved in striking the right balance between our security and our open society. As Commander-in Chief, I believe we must keep information secret that protects our operations and our people in the field. To do so, we must enforce consequences for those who break the law and breach their commitment to protect classified information. But a free press is also essential for our democracy. I am troubled by the possibility that leak investigations may chill the investigative journalism that holds government accountable.

Journalists should not be at legal risk for doing their jobs. Our focus must be on those who break the law. That is why I have called on Congress to pass a media shield law to guard against government over-reach. I have raised these issues with the Attorney General, who shares my concern. So he has agreed to review existing Department of Justice guidelines governing investigations that involve reporters, and will convene a group of media organizations to hear their concerns as part of that review. And I have directed the Attorney General to report back to me by July 12th.

All these issues remind us that the choices we make about war can impact – in sometimes unintended ways – the openness and freedom on which our way of life depends. And that is why I intend to engage Congress about the existing Authorization to Use Military Force, or AUMF, to determine how we can continue to fight terrorists without keeping America on a perpetual war-time footing.
The AUMF is now nearly twelve years old. The Afghan War is coming to an end. Core al Qaeda is a shell of its former self. Groups like AQAP must be dealt with, but in the years to come, not every collection of thugs that labels themselves al Qaeda will pose a credible threat to the United States. Unless we discipline our thinking and our actions, we may be drawn into more wars we don’t need to fight, or continue to grant Presidents unbound powers more suited for traditional armed conflicts between nation states. So I look forward to engaging Congress and the American people in efforts to refine, and ultimately repeal, the AUMF’s mandate. And I will not sign laws designed to expand this mandate further. Our systematic effort to dismantle terrorist organizations must continue. But this war, like all wars, must end. That’s what history advises. That’s what our democracy demands.

And that brings me to my final topic: the detention of terrorist suspects.

To repeat, as a matter of policy, the preference of the United States is to capture terrorist suspects. When we do detain a suspect, we interrogate them. And if the suspect can be prosecuted, we decide whether to try him in a civilian court or a Military Commission. During the past decade, the vast majority of those detained by our military were captured on the battlefield. In Iraq, we turned over thousands of prisoners as we ended the war. In Afghanistan, we have transitioned detention facilities to the Afghans, as part of the process of restoring Afghan sovereignty. So we bring law of war detention to an end, and we are committed to prosecuting terrorists whenever we can.

The glaring exception to this time-tested approach is the detention center at Guantanamo Bay. The original premise for opening GTMO – that detainees would not be able to challenge their detention – was found unconstitutional five years ago. In the meantime, GTMO has become a symbol around the world for an America that flouts the rule of law. Our allies won’t cooperate with us if they think a terrorist will end up at GTMO. During a time of budget cuts, we spend $150 million each year to imprison 166 people –almost $1 million per prisoner. And the Department of Defense estimates that we must spend another $200 million to keep GTMO open at a time when we are cutting investments in education and research here at home.

As President, I have tried to close GTMO. I transferred 67 detainees to other countries before Congress imposed restrictions to effectively prevent us from either transferring detainees to other countries, or imprisoning them in the United States. These restrictions make no sense. After all, under President Bush, some 530 detainees were transferred from GTMO with Congress’s support. When I ran for President the first time, John McCain supported closing GTMO. No person has ever escaped from one of our super-max or military prisons in the United States. Our courts have convicted hundreds of people for terrorism-related offenses, including some who are more dangerous than most GTMO detainees. Given my Administration’s relentless pursuit of al Qaeda’s leadership, there is no justification beyond politics for Congress to prevent us from closing a facility that should never have been opened.
Today, I once again call on Congress to lift the restrictions on detainee transfers from GTMO. I have asked the Department of Defense to designate a site in the United States where we can hold military commissions. I am appointing a new, senior envoy at the State Department and Defense Department whose sole responsibility will be to achieve the transfer of detainees to third countries. I am lifting the moratorium on detainee transfers to Yemen, so we can review them on a case by case basis. To the greatest extent possible, we will transfer detainees who have been cleared to go to other countries. Where appropriate, we will bring terrorists to justice in our courts and military justice system. And we will insist that judicial review be available for every detainee.

Even after we take these steps, one issue will remain: how to deal with those GTMO detainees who we know have participated in dangerous plots or attacks, but who cannot be prosecuted – for example because the evidence against them has been compromised or is inadmissible in a court of law. But once we commit to a process of closing GTMO, I am confident that this legacy problem can be resolved, consistent with our commitment to the rule of law.

I know the politics are hard. But history will cast a harsh judgment on this aspect of our fight against terrorism, and those of us who fail to end it. Imagine a future – ten years from now, or twenty years from now – when the United States of America is still holding people who have been charged with no crime on a piece of land that is not a part of our country. Look at the current situation, where we are force-feeding detainees who are holding a hunger strike. Is that who we are? Is that something that our Founders foresaw? Is that the America we want to leave to our children?

Our sense of justice is stronger than that. We have prosecuted scores of terrorists in our courts. That includes Umar Farouk Abdulmutallab, who tried to blow up an airplane over Detroit; and Faisal Shahzad, who put a car bomb in Times Square. It is in a court of law that we will try Dzhokhar Tsarnaev, who is accused of bombing the Boston Marathon. Richard Reid, the shoe bomber, is as we speak serving a life sentence in a maximum security prison here, in the United States. In sentencing Reid, Judge William Young told him, “the way we treat you...is the measure of our own liberties.” He went on to point to the American flag that flew in the courtroom – “That flag,” he said, “will fly there long after this is all forgotten. That flag still stands for freedom.”

America, we have faced down dangers far greater than al Qaeda. By staying true to the values of our founding, and by using our constitutional compass, we have overcome slavery and Civil War; fascism and communism. In just these last few years as President, I have watched the American people bounce back from painful recession, mass shootings, and natural disasters like the recent tornados that devastated Oklahoma. These events were heartbreaking; they shook our communities to the core. But because of the resilience of the American people, these events could not come close to breaking us.
I think of Lauren Manning, the 9/11 survivor who had severe burns over 80 percent of her body, who said, “That’s my reality. I put a Band-Aid on it, literally, and I move on.”

I think of the New Yorkers who filled Times Square the day after an attempted car bomb as if nothing had happened.

I think of the proud Pakistani parents who, after their daughter was invited to the White House, wrote to us, “we have raised an American Muslim daughter to dream big and never give up because it does pay off.”

I think of the wounded warriors rebuilding their lives, and helping other vets to find jobs.

I think of the runner planning to do the 2014 Boston Marathon, who said, “Next year, you are going to have more people than ever. Determination is not something to be messed with.”

That’s who the American people are. Determined, and not to be messed with.

Now, we need a strategy – and a politics – that reflects this resilient spirit. Our victory against terrorism won’t be measured in a surrender ceremony on a battleship, or a statue being pulled to the ground. Victory will be measured in parents taking their kids to school; immigrants coming to our shores; fans taking in a ballgame; a veteran starting a business; a bustling city street. The quiet determination; that strength of character and bond of fellowship; that refutation of fear – that is both our sword and our shield. And long after the current messengers of hate have faded from the world’s memory, alongside the brutal despots, deranged madmen, and ruthless demagogues who litter history – the flag of the United States will still wave from small-town cemeteries, to national monuments, to distant outposts abroad. And that flag will still stand for freedom.

Thank you. God Bless you. And may God bless the United States of America.

###
RULES OF PROCEDURE

FOR THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

(Adopted June 23, 1976)

(Amended June 26, 1987)

(Amended October 24, 1990)

(Amended February 25, 1993)

(Amended February 22, 1995)

(Amended January 26, 2005)

(Amended March 15, 2005)

(Amended March 1, 2007)
APPENDIX A

S. RES. 400, 94th Cong., 2d Sess. (1976)¹

Resolved, That it is the purpose of this resolution to establish a new select committee of the Senate, to be known as the Select Committee on Intelligence, to oversee and make continuing studies of the intelligence activities and programs of the United States Government, and to submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs. In carrying out this purpose, the Select Committee on Intelligence shall make every effort to assure that the appropriate departments and agencies of the United States provide informed and timely intelligence necessary for the executive and legislative branches to make sound decisions affecting the security and vital interests of the Nation. It is further the purpose of this resolution to provide vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States.

SEC. 2. (a)(1) There is hereby established a select committee to be known as the Select Committee on Intelligence (hereinafter in this resolution referred to as the "select committee"). The select committee shall be composed of not to exceed fifteen Members appointed as follows:

(A) two members from the Committee on Appropriations;
(B) two members from the Committee on Armed Services;
(C) two members from the Committee on Foreign Relations;
(D) two members from the Committee on the Judiciary; and
(E) not to exceed seven members to be appointed from the Senate at large.

(2) Members appointed from each committee named in clauses (A) through (D) of paragraph (1) shall be evenly divided between the two major political parties and shall be appointed by the President pro tempore of the Senate upon the recommendations of the majority and minority leaders of the Senate. Of any members appointed under paragraph (1)(E), the majority leader shall appoint the majority members and the minority leader shall appoint the minority members, with the majority having a one vote margin.

(3)(A) The majority leader of the Senate and the minority leader of the Senate shall be ex officio members of the select committee but shall have no vote in the Committee and shall not be counted for purposes of determining a quorum.

(B) The Chairman and Ranking Member of the Committee on Armed Services (if not already a member of the select Committee) shall be ex officio members of the select Committee but shall have no vote in the Committee and shall not be counted for purposes of determining a quorum.

(c) The select Committee may be organized into subcommittees. Each subcommittee shall have a chairman and a vice chairman who are selected by the Chairman and Vice Chairman of the select Committee, respectively.

SEC. 3. (a) There shall be referred to the select committee all proposed legislation, messages, petitions, memorials, and other matters relating to the following:

(1) The Office of the Director of National Intelligence and the Director of National Intelligence.

(2) The Central Intelligence Agency and the Director of the Central Intelligence Agency.

(3) Intelligence activities of all other departments and agencies of the Government, including, but not limited to, the intelligence activities of the Defense Intelligence Agency, the National Security Agency, and other agencies of the Department of Defense; the Department of State; the Department of Justice; and the Department of the Treasury.

(4) The organization or reorganization of any department or agency of the Government to the extent that the organization or reorganization relates to a function or activity involving intelligence activities.

(5) Authorizations for appropriations, both direct and indirect, for the following:

(A) The Office of the Director of National Intelligence and the Director of National Intelligence.
(B) The Central Intelligence Agency and the Director of the Central Intelligence Agency.
(C) The Defense Intelligence Agency.
(D) The National Security Agency.
(E) The intelligence activities of other agencies and subdivisions of the Department of Defense.
(F) The intelligence activities of the Department of State.
(G) The intelligence activities of the Federal Bureau of Investigation.
(H) Any department, agency, or subdivision which is the successor to any agency named in clause (A), (B), (C) or (D); and the activities of any department, agency, or subdivision which is the successor to any department, agency, bureau, or subdivision named in clause (E), (F), or (G) to the extent that the activities of such successor department, agency, or subdivision are activities described in clause (E), (F), or (G).

(b) Any proposed legislation reported by the select Committee except any legislation involving matters specified in clause (1), (2), (5)(A), or (5)(B) of subsection (a), containing any matter otherwise within the jurisdiction of any standing committee, shall, at the request of the chairman of such standing committee, be referred to such standing committee for its consideration of such matter and be reported to the Senate by such standing committee within 10 days after the day on which such proposed legislation, in its entirety and including annexes, is referred to such standing committee; and any proposed legislation reported by any committee other than the select Committee, which contains any matter within the jurisdiction of the select Committee, shall, at the request of the chairman of the select Committee, be referred to the select Committee for its consideration of such matter and be reported to the Senate by the select Committee within 10 days after the day on which such proposed legislation, in its entirety and including annexes, is referred to such committee.

(2) In any case in which a committee fails to report any proposed legislation referred to it within the time limit prescribed in this subsection, such Committee shall be automatically discharged from further consideration of such proposed legislation on the 10th day following the day on which such proposed legislation is referred to such committee unless the Senate provides otherwise, or the Majority Leader or Minority Leader request, prior to that date, an additional 5 days on behalf of the Committee to which the proposed legislation was sequentially referred. At the end of that additional 5 day period, if the Committee fails to report the proposed legislation within that 5 day period, the Committee shall be automatically discharged from further consideration of such proposed legislation unless the Senate provides otherwise.

(3) In computing any 10 or 5 day period under this subsection there shall be excluded from such computation any days on which the Senate is not in session.

(c) Nothing in this resolution shall be construed as prohibiting or otherwise restricting the authority of any other committee to study and review any intelligence activity to the extent that such activity directly affects a matter otherwise within the jurisdiction of such committee.

(d) Nothing in this resolution shall be construed as amending, limiting, or otherwise changing the authority of any standing committee of the Senate to obtain full and prompt access to the products of the intelligence activities of any department or agency of the Government relevant to a matter otherwise within the jurisdiction of such committee.

SEC. 4. (a) The select committee, for the purposes of accountability to the Senate, shall make regular and periodic, but not less than quarterly, reports to the Senate
on the nature and extent of the intelligence activities of the various departments and agencies of the United States. Such committee shall promptly call to the attention of the Senate or to any other appropriate committee or committees of the Senate any matters requiring the attention of the Senate or such other committee or committees. In making such report, the select committee shall proceed in a manner consistent with section 8(c)(2) to protect national security.

(b) The select committee shall obtain an annual report from the Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of Defense, the Secretary of State, and the Director of the Federal Bureau of Investigation. Such reports shall review the intelligence activities of the agency or department concerned and the intelligence activities of foreign countries directed at the United States or its interest. An unclassified version of each report may be made available to the public at the discretion of the select committee. Nothing herein shall be construed as requiring the public disclosure in such reports of the names of individuals engaged in intelligence activities for the United States or the divulging of intelligence methods employed or the sources of information on which such reports are based or the amount of funds authorized to be appropriated for intelligence activities.

(c) On or before March 15 of each year, the select committee shall submit to the Committee on the Budget of the Senate the views and estimates described in section 301(c) of the Congressional Budget Act of 1974 regarding matters within the jurisdiction of the select committee.

Sec. 5. (a) For the purposes of this resolution, the select committee is authorized in its discretion (1) to make investigations into any matter within its jurisdiction, (2) to make expenditures from the contingent fund of the Senate, (3) to employ personnel, (4) to hold hearings, (5) to sit and act at any time or place during the sessions, recesses, and adjourned periods of the Senate, (6) to require, by subpoena or otherwise, the attendance of witnesses and the production of correspondence, books, papers, and documents, (7) to take depositions and other testimony, (8) to procure the service of individual consultants or organizations thereof, in accordance with the provisions of section 202(n) of the Legislative Reorganization Act of 1946, and (9) with the prior consent of the government department or agency concerned and the Committee on Rules and Administration, to use on a reimbursable basis the services of personnel of any such department or agency.

(b) The chairman of the select committee or any member thereof may administer oaths to witnesses.

(c) Subpoenas authorized by the select committee may be issued over the signature of the chairman, the vice chairman, or any member of the select committee designated by the chairman, and may be served by any person designated by the chairman or any member signing the subpoenas.

Sec. 6. No employee of the select committee or any person engaged by contract or otherwise to perform services for or at the request of such committee shall be given access to any classified information by such committee unless such employee or person has (1) agreed in writing and under oath to be bound by the rules of the Senate (including the jurisdiction of the Select Committee on Ethics) and of such committee as to the security of such information during and after the period of his employment or contractual agreement with such committee; and (2) received an appropriate security clearance as determined by such committee in consultation with the Director of National Intelligence. The type of security clearance to be required in the case of any such employee or person shall, within the determination of such committee in consultation with the Director of National Intelligence, be commensurate with the sensitivity of the classified information to which such employee or person will be given access by such committee.

Sec. 7. The select committee shall formulate and carry out such rules and procedures as it deems necessary to prevent the disclosure, without the consent of the person or persons concerned, of information in the possession of such committee which unduly infringes upon the privacy or which violates the constitutional rights of such person or persons. Nothing herein shall be construed to prevent such committee from publicly disclosing any such information in any case in which such committee determines the national interest in the disclosure of such information clearly outweighs any infringement on the privacy of any person or persons.

Sec. 8. (a) The select committee may, subject to the provisions of this section, disclose publicly any information in the possession of such committee after a determination by such committee that the public interest would be served by such disclosure. Whenever committee action is required to disclose any information under this section, the committee shall meet to vote on the matter within five days after any member of the committee requests such a vote. No member of the select committee shall disclose any information, the disclosure of which requires a committee vote,
prior to a vote by the committee on the question of the disclosure of such information or after such vote except in accordance with this section.

(b)(1) In any case in which the select committee votes to disclose publicly any information which has been classified under established security procedures, which has been submitted to it by the Executive branch, and which the Executive branch requests be kept secret, such committee shall—
(A) first, notify the Majority Leader and Minority Leader of the Senate of such vote; and
(B) second, consult with the Majority Leader and Minority Leader before notifying the President of such vote.

(2) The select committee may disclose publicly such information after the expiration of a five-day period following the day on which notice of such vote is transmitted to the Majority Leader and the Minority Leader and the President, unless, prior to the expiration of such five-day period, the President, personally in writing, notifies the committee that he objects to the disclosure of such information, provides his reasons therefore, and certifies that the threat to the national interest of the United States posed by such disclosure is of such gravity that it outweighs any public interest in the disclosure.

(3) If the President, personally, in writing, notifies the Majority Leader and Minority Leader of the Senate and the select Committee of his objections to the disclosure of such information as provided in paragraph (2), the Majority Leader and Minority Leader jointly or the select Committee, by majority vote, may refer the question of the disclosure of such information to the Senate for consideration.

(4) Whenever the select committee votes to refer the question of disclosure of any information to the Senate under paragraph (3), the Chairman shall act not later than the first day on which the Senate is in session following the day on which the vote occurs, report the matter to the Senate for its consideration.

(5) One hour after the Senate convenes on the fourth day on which the Senate is in session following the day on which any such matter is reported to the Senate, or at such earlier time as the majority leader and the minority leader of the Senate jointly agree upon in accordance with paragraph 5 of rule XVII of the Standing Rules of the Senate, the Senate shall go into closed session and the matter shall be the pending business. In considering the matter in closed session the Senate may—
(A) approve the public disclosure of all or any portion of the information in question, in which case the committee shall publicly disclose the information ordered to be disclosed,
(B) disapprove the public disclosure of all or any portion of the information in question, in which case the committee shall not publicly disclose the information ordered not to be disclosed, or
(C) refer all or any portion of the matter back to the committee, in which case the committee shall make the final determination with respect to the public disclosure of the information in question.

Upon conclusion of the consideration of such matter in closed session, which may not extend beyond the close of the ninth day on which the Senate is in session following the day on which such matter was reported to the Senate, or the close of the fifth day following the day agreed upon jointly by the majority and minority leaders in accordance with paragraph 5 of rule XVII of the Standing Rules of the Senate (whichever the case may be), the Senate shall immediately vote on the disposition of such matter in open session, without debate, and without divulging the information with respect to which the vote is being taken. The Senate shall vote to dispose of such matter by one or more of the means specified in clauses (A), (B), and (C) of the second sentence of this paragraph. Any vote of the Senate to disclose any information pursuant to this paragraph shall be subject to the right of a Member of the Senate to move for reconsideration of the vote within the time and pursuant to the procedures specified in rule XIII of the Standing Rules of the Senate, and the disclosure of such information shall be made consistent with that right.

(c)(1) No information in the possession of the select committee relating to the lawful intelligence activities of any department or agency of the United States which has been classified under established security procedures and which the select committee, pursuant to subsection (a) or (b) of this section, has determined should not be disclosed shall be made available to any person by a Member, officer, or employee of the Senate except in a closed session of the Senate or as provided in paragraph (2).

(2) The select committee may, under such regulations as the committee shall prescribe to protect the confidentiality of such information, make any information described in paragraph (1) available to any other committee or any other Member of the Senate. Whenever the select committee makes such information available, the
committee shall keep a written record showing, in the case of any particular information, which committee or which Members of the Senate received such information. No Member of the Senate who, and no committee which, receives any information under this subsection, shall disclose such information except in a closed session of the Senate.

(d) It shall be the duty of the Select Committee on Ethics to investigate any unauthorized disclosure of intelligence information by a Member, officer or employee of the Senate in violation of subsection (c) and to report to the Senate concerning any allegation which it finds to be substantiated.

(e) Upon the request of any person who is subject to any such investigation, the Select Committee on Ethics shall release to such individual at the conclusion of its investigation a summary of its investigation together with its findings. If, at the conclusion of its investigation, the Select Committee on Ethics determines that there has been a significant breach of confidentiality or unauthorized disclosure by a Member, officer, or employee of the Senate, it shall report its findings to the Senate and recommend appropriate action such as censure, removal from committee membership, or expulsion from the Senate, in the case of a Member, or removal from office or employment or punishment for contempt, in the case of an officer or employee.

SEC. 9. The select committee is authorized to permit any personal representative of the President, designated by the President to serve as a liaison to such committee, to attend any closed meeting of such committee.

SEC. 10. Upon expiration of the Select Committee on Governmental Operations With Respect to Intelligence Activities, established by Senate Resolution 21, Ninety-fourth Congress, all records, files, documents, and other materials in the possession, custody, or control of such committee, under appropriate conditions established by it, shall be transferred to the select committee.

SEC. 11. (a) It is the sense of the Senate that the head of each department and agency of the United States should keep the select committee fully and currently informed with respect to intelligence activities, including any significant anticipated activities, which are the responsibility of or engaged in by such department or agency: Provided, That this does not constitute a condition precedent to the implementation of any such anticipated intelligence activity.

(b) It is the sense of the Senate that the head of any department or agency of the United States involved in any intelligence activities should furnish any information or document in the possession, custody, or control of the department or agency, or person paid by such department or agency, whenever requested by the select committee with respect to any matter within such committee's jurisdiction.

(c) It is the sense of the Senate that each department and agency of the United States should report immediately upon discovery to the select committee any and all intelligence activities which constitute violations of the constitutional rights of any person, violations of law, or violations of Executive orders, Presidential directives, or departmental or agency rules or regulations; each department and agency should further report to such committee what actions have been taken or are expected to be taken by the departments or agencies with respect to such violations.

SEC. 12. Subject to the Standing Rules of the Senate, no funds shall be appropriated for any fiscal year beginning after September 30, 1976, with the exception of a continuing bill or resolution, or amendment thereto, or conference report thereon, to, or for use of, any department or agency of the United States to carry out any of the following activities, unless such funds shall have been previously authorized by a bill or joint resolution passed by the Senate during the same or preceding fiscal year to carry out such activity for such fiscal year:

(1) The activities of the Office of the Director of National Intelligence and the Director of National Intelligence.

(2) The activities of the Central Intelligence Agency and the Director of the Central Intelligence Agency.

(3) The activities of the Defense Intelligence Agency.

(4) The activities of the National Security Agency.

(5) The intelligence activities of other agencies and subdivisions of the Department of Defense.

(6) The intelligence activities of the Department of State.

SEC. 13. (a) The select committee shall make a study with respect to the following matters, taking into consideration with respect to each such matter, all relevant aspects of the effectiveness of planning, gathering, use, security, and dissemination of intelligence:
(1) the quality of the analytical capabilities of United States foreign intelligence agencies and means for integrating more closely analytical intelligence and policy formulation;

(2) the extent and nature of the authority of the departments and agencies of the Executive branch to engage in intelligence activities and the desirability of developing charters for each intelligence agency or department;

(3) the organization of intelligence activities in the Executive branch to maximize the effectiveness of the conduct, oversight, and accountability of intelligence activities; to reduce duplication or overlap; and to improve the morale of the personnel of the foreign intelligence agencies;

(4) the conduct of covert and clandestine activities and the procedures by which Congress is informed of such activities;

(5) the desirability of changing any law, Senate rule or procedure, or any Executive order, rule, or regulation to improve the protection of intelligence secrets and provide for disclosure of information for which there is no compelling reason for secrecy;

(6) the desirability of establishing a standing committee of the Senate on intelligence activities;

(7) the desirability of establishing a joint committee of the Senate and the House of Representatives on intelligence activities in lieu of having separate committees in each House of Congress, or of establishing procedures under which separate committees on intelligence activities of the two Houses of Congress would receive joint briefings from the intelligence agencies and coordinate their policies with respect to the safeguarding of sensitive intelligence information;

(8) the authorization of funds for the intelligence activities of the Government and whether disclosure of any of the amounts of such funds is in the public interest; and

(9) the development of a uniform set of definitions for terms to be used in policies or guidelines which may be adopted by the executive or legislative branches to govern, clarify, and strengthen the operation of intelligence activities.

(b) The select Committee may, in its discretion, omit from the special study required by this section any matter it determines has been adequately studied by the Select Committee To Study Governmental Operations With Respect to Intelligence Activities, established by Senate Resolution 21, Ninety-fourth Congress.

(c) The select committee shall report the results of the study provided for by this section to the Senate, together with any recommendations for legislative or other actions it deems appropriate, no later than July 1, 1977, and from time to time thereafter as it deems appropriate.

SEC. 14. (a) As used in this resolution, the term "intelligence activities" includes (1) the collection, analysis, production, dissemination, or use of information which relates to any foreign country, or any government, political group, party, military force, movement, or other association in such foreign country, and which relates to the defense, foreign policy, national security, or related policies of the United States, and other activity which is in support of such activities; and (2) activities taken to counter similar activities directed against the United States; (3) covert or clandestine activities affecting the relations of the United States with any foreign government, political group, party, military force, movement or other association; (4) the collection, analysis, production, dissemination, or use of information about activities of persons within the United States, its territories and possessions, or nationals of the United States abroad whose political and related activities pose, or may be considered by any department, agency, bureau, office, division, instrumentality, or employee of the United States to pose, a threat to the internal security of the United States, and covert or clandestine activities directed against such persons. Such term does not include tactical foreign military intelligence serving no national policymaking function.

(b) As used in this resolution, the term "department or agency" includes any organization, committee, council, establishment, or office within the Federal Government.

(c) For purposes of this resolution, reference to any department, agency, bureau, or subdivision shall include a reference to any successor department, agency, bureau, or subdivision to the extent that such successor engages in intelligence activities now conducted by the department, agency, bureau, or subdivision referred to in this resolution.

SEC. 15. (a) In addition to other committee staff selected by the select Committee, the select Committee shall hire or appoint one employee for each member of the select Committee to serve as such Member's designated representative on the select
Committee. The select Committee shall only hire or appoint an employee chosen by the respective Member of the select Committee for whom the employee will serve as the designated representative on the select Committee.

(b) The select Committee shall be afforded a supplement to its budget, to be determined by the Committee on Rules and Administration, to allow for the hire of each employee who fills the position of designated representative to the select Committee. The designated representative shall have office space and appropriate office equipment in the select Committee spaces. Designated personal representatives shall have the same access to Committee staff, information, records, and databases as select Committee staff, as determined by the Chairman and Vice Chairman.

(c) The designated employee shall meet all the requirements of relevant statutes, Senate rules, and committee security clearance requirements for employment by the select Committee.

(d) Of the funds made available to the select Committee for personnel—

(1) not more than 60 percent shall be under the control of the Chairman; and

(2) not less than 40 percent shall be under the control of the Vice Chairman.

SEC. 16. Nothing in this resolution shall be construed as constituting acquiescence by the Senate in any practice, or in the conduct of any activity, not otherwise authorized by law.

SEC. 17. (a)(1) Except as otherwise provided in subsection (b), the select Committee shall have jurisdiction for reviewing, holding hearings, and reporting the nominations of civilian persons nominated by the President to fill all positions within the intelligence community requiring the advice and consent of the Senate.

(2) Other committees with jurisdiction over the nominees' executive branch department may hold hearings and interviews with such persons, but only the select Committee shall report such nominations.

(b)(1) With respect to the confirmation of the Assistant Attorney General for National Security, or any successor position, the nomination of any individual by the President to serve in such position shall be referred to the Committee on the Judiciary and, if and when reported, to the select Committee for not to exceed 20 calendar days, except that in cases when the 20-day period expires while the Senate is in recess, the select Committee shall have 5 additional calendar days after the Senate reconvenes to report the nomination.

(2) If, upon the expiration of the period described in paragraph (1), the select Committee has not reported the nomination, such nomination shall be automatically discharged from the select Committee and placed on the Executive Calendar.
APPENDIX B
WERE NOT INCORPORATED IN S. RES. 400, 94TH CONG., 2D SESS. (1976)

TITLE III—COMMITTEE STATUS

SEC. 301(b) INTELLIGENCE.—The Select Committee on Intelligence shall be treated
as a committee listed under paragraph 2 of rule XXV of the Standing Rules of the
Senate for purposes of the Standing Rules of the Senate.

TITLE IV—INTELLIGENCE-RELATED SUBCOMMITTEES

SEC. 401. SUBCOMMITTEE RELATED TO INTELLIGENCE OVERSIGHT.
(a) ESTABLISHMENT.—There is established in the Select Committee on Intelligence
a Subcommittee on Oversight which shall be in addition to any other subcommittee
established by the select Committee.
(b) RESPONSIBILITY.—The Subcommittee on Oversight shall be responsible for on-
going oversight of intelligence activities.

SEC. 402. SUBCOMMITTEE RELATED TO INTELLIGENCE APPROPRIATIONS.
(a) ESTABLISHMENT.—There is established in the Committee on Appropriations a
Subcommittee on Intelligence. The Committee on Appropriations shall reorganize
into 13 subcommittees as soon as possible after the convening of the 109th Con-
gress.
(b) JURISDICTION.—The Subcommittee on Intelligence of the Committee on Approp-
rations shall have jurisdiction over funding for intelligence matters, as determined
by the Senate Committee on Appropriations.
APPENDIX C
RULE 26.5(b) OF THE STANDING RULES OF THE SENATE

(REFERRED TO IN COMMITTEE RULE 2.1)

Each meeting of a committee, or any subcommittee thereof, including meetings to conduct hearings, shall be open to the public, except that a meeting or series of meetings by a committee or a subcommittee thereof on the same subject for a period of no more than fourteen calendar days may be closed to the public on a motion made and seconded to go into closed session to discuss only whether the matters enumerated in clauses (1) through (6) would require the meeting to be closed, followed immediately by a record vote in open session by a majority of the members of the committee or subcommittee when it is determined that the matters to be discussed or the testimony to be taken at such meeting or meetings—

(1) will disclose matters necessary to be kept secret in the interests of national defense or the confidential conduct of the foreign relations of the United States;
(2) will relate solely to matters of committee staff personnel or internal staff management or procedure;
(3) will tend to charge an individual with crime or misconduct, to disgrace or injure the professional standing of an individual, or otherwise to expose an individual to public contempt or obloquy, or will represent a clearly unwarranted invasion of the privacy of an individual;
(4) will disclose the identity of any informer or law enforcement agent or will disclose any information relating to the investigation or prosecution of a criminal offense that is required to be kept secret in the interests of effective law enforcement;
(5) will disclose information relating to the trade secrets of financial or commercial information pertaining specifically to a given person if—
   (A) an Act of Congress requires the information to be kept confidential by Government officers and employees; or
   (B) the information has been obtained by the Government or a confidential basis, other than through an application by such person for a specific Government financial or other benefit, and is required to be kept secret in order to prevent undue injury to the competitive position of such person; or
(6) may divulge matters required to be kept confidential under other provisions of law or Government regulations.
LUNCHEON DISCUSSION:

CRITICAL NATIONAL SECURITY CASES TO WATCH

DISCUSSANTS:
MIGUEL ESTRADA & PRATIK SHAH
of bringing a collective action does not mean that individual attempts at conciliation were intended to be barred. Id. at 32, 111 S.Ct. 1647 (internal quotation marks omitted). As the passage from Gilmer reflects, the ADEA expressly provides for a collective action; a fortiori, the same result obtains under the antitrust laws, which do not. The only right to an antitrust class action is “merely a procedural one, arising under Fed.R.Civ.P. 23, that may be waived by agreeing to an arbitration clause.” Johnson v. W. Suburban Bank, 225 F.3d 366, 369 (3d Cir.2000) (enforcing, due to absence of congressional intent to the contrary, a bilateral arbitration clause “even though [such clauses] may render class actions to pursue statutory claims . . . unavailable”).

JOSE A. CABRANES, Circuit Judge, dissenting from the denial of rehearing en banc:

I concur fully in the thorough opinion of Chief Judge Jacobs dissenting from the denial of en banc review. I write separately simply to underscore that the issue at hand is indisputably important, creates a circuit split, and surely deserves further appellate review. This is one of those unusual cases where one can infer that the denial of en banc review can only be explained as a signal that the matter can and should be resolved by the Supreme Court.

REENA RAGGI, Circuit Judge, with whom Judge WESLEY joins, dissenting from the denial of rehearing en banc:

I respectfully dissent from the denial of en banc review in this case. The panel decision to hold a class action waiver unenforceable is at odds with Coney v. AT & T Corp., 673 F.3d 1155 (9th Cir.2012). This circuit split appears unwarranted in light of controlling Supreme Court precedent for the reasons forcefully advanced by Chief Judge Jacobs in his opinion dissenting from the denial of rehearing en banc. While I identify much merit in the Chief Judge’s analysis, I do not join in his opinion because I think it would be useful to have the issues explored further by the full court in the adversarial context of an en banc argument. To the extent a majority of the court maintains this circuit split without further consideration, I must dissent.

UNITED STATES of America
v.
Carol Anne BOND, Appellant.

No. 08–2677.

United States Court of Appeals,
Third Circuit.

Argued Nov. 16, 2011.

Filed: May 3, 2012.

Background: Defendant was convicted by guilty plea in the United States District Court for the Eastern District of Pennsylvania, James T. Giles, J., of possessing and using a chemical weapon and mail theft, and she appealed. The Court of Appeals, Ambro, Circuit Judge, 581 F.3d 128, affirmed, and certiorari was granted. The Supreme Court, Justice Kennedy, U.S. ——, 131 S.Ct. 2355, 180 L.Ed.2d 269, reversed and remanded.

Holding: On remand, the Court of Appeals, Jordan, Circuit Judge, held that Chemical Weapons Convention Implementation Act did not exceed Congress’ power under Necessary and Proper Clause. Affirmed.
Rendell, Circuit Judge, filed a concurring opinion.

Ambro, Circuit Judge, filed a separate concurring opinion.

1. Weapons ⇔111

Defendant’s use of highly toxic chemicals with intent to harm a former friend did not fall under Chemical Weapons Convention Implementation Act’s peaceful purpose exception; defendant’s use of chemicals was not related to an industrial, agricultural, research, medical, or pharmaceutical activity, as contemplated by exception. 18 U.S.C.A. § 229(a)(1).

2. Treaties ⇔7

United States ⇔22

When there is a valid treaty, Congress has authority to enact implementing legislation under the Necessary and Proper Clause, even if it might otherwise lack the ability to legislate in the domain in question; however, the legislation must meet the Clause’s general requirement that legislation implemented under that Clause be rationally related to the implementation of a constitutionally enumerated power. U.S.C.A. Const. Art. 1, § 8, cl. 18.

3. States ⇔4.16(2)

Treaties ⇔11

As long as the effectuating legislation bears a rational relationship to a valid treaty under the Necessary and Proper Clause, the treaty and associated legislation are simply not subject to Tenth Amendment scrutiny, no matter how far into the realm of states’ rights the President and Congress may choose to venture. U.S.C.A. Const. Art. 1, § 8, cl. 18; U.S.C.A. Const. Art. 2, § 2, cl. 2; U.S.C.A. Const.Amend. 10.

4. United States ⇔22

Chemical Weapons Convention Implementation Act, which makes it unlawful for any person knowingly to develop, produce, possess, or use, any chemical weapon, was a valid exercise of congressional power under Necessary and Proper Clause; Act closely adhered to, and did not materially expand, language of Convention. U.S.C.A. Const. Art. 1, § 8, cl. 18; 18 U.S.C.A. § 229(a)(1).


Paul G. Shapiro [Argued], Office of United States Attorney, Philadelphia, PA, for Appellee.

Before: RENDELL, AMBRO, and JORDAN, Circuit Judges.

OPINION OF THE COURT

JORDAN, Circuit Judge.

This case is before us on remand from the Supreme Court, which vacated our earlier judgment that Appellant Carol Anne Bond lacked standing to challenge, on Tenth Amendment grounds, her conviction under the penal provision of the Chemical Weapons Convention Implementation Act of 1998, 18 U.S.C. § 229 (the “Act”), which implements the 1993 Chemical Weapons Convention, 32 I.L.M. 800 (1993) (the “Convention”). The Supreme Court determined that Bond does have standing to advance that challenge, and returned the
case to us to consider her constitutional argument.

In her merits argument, Bond urges us to set aside as inapplicable the landmark decision Missouri v. Holland, 252 U.S. 416, 40 S.Ct. 382, 64 L.Ed. 641 (1920), which is sometimes cited for the proposition that the Tenth Amendment has no bearing on Congress's ability to legislate in furtherance of the Treaty Power in Article II, § 2 of the Constitution. Cognizant of the widening scope of issues taken up in international agreements, as well as the renewed vigor with which principles of federalism have been employed by the Supreme Court in scrutinizing assertions of federal authority, we agree with Bond that treaty-implementing legislation ought not, by virtue of that status alone, stand immune from scrutiny under principles of federalism. However, because the Convention is an international agreement with a subject matter that lies at the core of the Treaty Power and because Holland instructs that "there can be no dispute about the validity of [a] statute" that implements a valid treaty, 252 U.S. at 432, 40 S.Ct. 382, we will affirm Bond's conviction.

I. Factual Background and Procedural History

A. Facts

Bond's criminal acts are detailed in our prior opinion, United States v. Bond, 581 F.3d 128, 131–33 (3d Cir.2009) ("Bond I"), and in the Supreme Court's opinion, Bond v. United States, — U.S. —, 131 S.Ct. 2355, 2360–61, 180 L.Ed.2d 269 (2011) ("Bond II"), so we provide only a brief recitation here. Suffice it to say that, while Bond was employed by the chemical manufacturer Rohm and Haas, she learned that her friend Myrlinda Haynes was pregnant and that Bond's own husband was the baby's father. Bond became intent on revenge. To that end, she set about acquiring highly toxic chemicals, stealing 10-chlorophenoxarsine from her employer and purchasing potassium dichromate over the Internet. She then applied those chemicals to Haynes's mailbox, car door handles, and house doorknob. Bond's poisonous activities were eventually discovered and she was indicted on two counts of acquiring, transferring, receiving, retaining, or possessing a chemical weapon, in violation of the Act. She was, in addition, charged with two counts of theft of mail matter, in violation of 18 U.S.C. § 1708.

B. Procedural History

Bond filed a motion to dismiss the counts that alleged violations of the Act. She argued that the Act was unconstitutional, both facially and as applied to her. More particularly, she said that the Act violated constitutional "fair notice" requirements, that it was inconsistent with the Convention it was meant to implement, and that it represented a breach of the Tenth Amendment's protection of state sovereignty. Emphasizing that last point, Bond contended that neither the Commerce Clause, nor the Necessary and Proper Clause in connection with the Treaty Power, could support the expansive wording of the statute, i.e., alone her prosecution. (See App. at 59 (arguing that, "[g]iven the localized . . . scope of the conduct alleged, . . . application of 18 U.S.C. § 229 signals a massive and unjustifiable expansion of federal law enforcement into state-regulated domain").) The government's response has shifted over time,¹ but

¹. The government has, at different stages of this case, been willing to jettison one legal position and adopt a different one, as seemed convenient. Before the District Court, it expressly disclaimed the Commerce Clause as a basis for Congress's power to approve the Act.
it has been consistent in maintaining that the Act is a constitutional exercise of Congress’s authority to enact treaty-implementing legislation under the Necessary and Proper Clause. The District Court accepted that argument and denied Bond’s motion to dismiss.

We affirmed on appeal, concluding that Bond lacked standing to pursue her Tenth Amendment challenge and that the Act was neither unconstitutionally vague nor unconstitutionally overbroad.2 Bond I, 581 F.3d at 139. The Supreme Court granted certiorari to address the question of “whether a criminal defendant convicted under a federal statute has standing to challenge her conviction on grounds that, as applied to her, the statute is beyond the federal government’s enumerated powers and inconsistent with the Tenth Amendment.” Petition for Writ of Certiorari, Bond v. United States (No. 09–1227), 2010 WL 1506717 at *i; see Bond v. United States, — U.S. —, 131 S.Ct. 455, 178 L.Ed.2d 285 (2010). Ultimately, the Court concluded that Bond “does have standing to challenge the federal statute.” Bond II, 131 S.Ct. at 2360. The case was remanded to us to address the “issue of the statute’s validity” which, as the Court instructed, “turns in part on whether the law can be deemed necessary and proper for carrying into Execution the President’s Article II, § 2 Treaty Power.” Id. at 2367 (quoting U.S. Const. art. I, § 8, cl. 18).

II. Discussion3

In Missouri v. Holland, the Supreme Court declared that, if a treaty is valid, “there can be no dispute about the validity of the statute [implementing it] under Article 1, Section 8, as a necessary and proper means to execute the powers of the Government.” 4 252 U.S. at 432, 40 S.Ct. S.Ct. 366, 83 L.Ed. 543 (1939), which held that “appellants, absent the states or their officers, have no standing . . . to raise any question under the [Tenth] [A]mendment,” id. at 144, 59 S.Ct. 366. (United States v. Bond, No. 08–2677, 08/20/2009 Letter from Appellee.) Before the Supreme Court, however, the government reversed course and argued that Bond did have standing to make a Tenth Amendment challenge. See Bond II, 131 S.Ct. at 2361 (describing the government’s initial “position that Bond did not have standing” and the changed position before the Supreme Court that “Bond does have standing”).

2. We determined that Bond lacked standing to pursue her Tenth Amendment challenge after requesting supplemental briefing on the question of whether the “ha[d] standing to assert that 18 U.S.C. § 229 encroaches on state sovereignty in violation of the Tenth Amendment to the United States Constitution absent the involvement of a state or its instrumentalities.” (United States v. Bond, No. 08–2677, 08/14/2009 Letter to Counsel.) The government responded that Bond lacked such standing under Tennessee Electric Power Co. v. Tennessee Valley Authority, 306 U.S. 118, 59 S.Ct. 366, 83 L.Ed. 543 (1939), which held that “appellants, absent the states or their officers, have no standing . . . to raise any question under the [Tenth] [A]mendment,” id. at 144, 59 S.Ct. 366. (United States v. Bond, No. 08–2677, 08/20/2009 Letter from Appellee.) Before the Supreme Court, however, the government reversed course and argued that Bond did have standing to make a Tenth Amendment challenge. See Bond II, 131 S.Ct. at 2361 (describing the government’s initial “position that Bond did not have standing” and the changed position before the Supreme Court that “Bond does have standing”).

3. The District Court had jurisdiction under 18 U.S.C. § 3231. We have jurisdiction under 28 U.S.C. § 1291 and 18 U.S.C. § 3742, and review de novo a challenge to the constitutionality of a criminal statute, Bond I, 581 F.3d at 133.

4. The referenced section of the Constitution is the Necessary and Proper Clause, which provides Congress with the power “[t]o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitu-
382. Implicit in that statement is the premise that principles of federalism will ordinarily impose no limitation on Congress’s ability to write laws supporting treaties, because the only relevant question is whether the underlying treaty is valid. See id. at 432, 434, 40 S.Ct. 382 (stating that “it is not enough to refer to the Tenth Amendment, reserving the powers not delegated to the United States” because the Treaty Power is delegated, but acknowledging the possibility that there may sometimes be “invisible radiation[s] from the general terms of the Tenth Amendment”). Reasoning that a reading of Holland that categorically rejects federalism as a check on Congress’s treaty-implementing authority is of questionable constitutional validity, Bond asks us to invalidate her conviction because the Act is unconstitutional as applied to her. She says that to hold otherwise would offend the Constitution’s balance of power between state and federal authority by “intrud[ing] . . . on the traditional state prerogative to punish assaults.” (Appellant’s Supp. Br. at 47.)

A. Constitutional Avoidance

Bond first argues, however, that we should avoid reaching the constitutional question by construing the Act not to apply to her conduct at all.6

[1] Her avoidance argument begins with the text of the Act itself, which provides, in pertinent part, that “it shall be unlawful for any person knowingly . . . to develop, produce, otherwise acquire, transfer directly or indirectly, receive, stockpile, retain, own, possess, or use, or threaten to use, any chemical weapon.” 18 U.S.C. § 229(a)(1). The term “chemical weapon” is defined broadly to include any “toxic chemical and its precursors,” id. § 229F(1)(A), and “[t]he term ‘toxic chemical’ means any chemical which through its chemical action on life processes can cause death, temporary incapacitation or perma-

5. It appears that Bond has abandoned her facial challenge to the Act. Her argument, both in her supplemental briefing before us and at oral argument, is articulated as an as-applied challenge. (See, e.g., Appellant’s Supp. Br. at 26 (“Bond is raising a . . . limited and narrowly focused as-applied challenge. She contends that, whatever its validity more generally, the statute cannot be constitutionally applied to her in the circumstances of this case.”); Transcript of Oral Argument at 11–13. United States v. Bond, No. 08–2677 (“3d Cir. Argument”).) And, Bond’s counsel commented at oral argument that he was “trying . . . [to be] respectful of the Supreme Court’s jurisprudence that says you don’t lightly bring a facial challenge” to a statute. (3d Cir. Argument at 62.) Counsel framed his argument as being that “the principle[] that [the statute has] offended is that if you apply it so broadly that it criminalizes every malicious use of poisoning, then you’ve overridden the structural limitations on the government and the division of power between the federal government and the states.” (Id. at 15–16.) We thus take it as granted that, although some of her past arguments move into the territory of a facial challenge, Bond is not now saying that Congress was without power to pass the Act but is, instead, arguing that Congress could not properly pass it if the Act’s language is interpreted in a way that reaches her conduct. In short, we are dealing with an as-applied, rather than a facial, challenge.

6. Bond’s constitutional avoidance argument necessarily presumes a serious constitutional problem, notwithstanding Holland. See Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council, 485 U.S. 568, 575, 108 S.Ct. 1392, 99 L.Ed.2d 645 (1988) (stating the constitutional avoidance inquiry should be undertaken in the face of “serious constitutional problems”). Regardless of Holland’s breadth, we accept Bond’s suggestion that it is prudent to begin our analysis with the avoidance doctrine.
nent harm to humans or animals,” id. § 229F(8)(A). Congress did put some limit on the sweep of the Act by excluding from the definition of “chemical weapon” any chemicals and precursors “intended for a purpose not prohibited under this chapter as long as the type and quantity is consistent with such a purpose.” Id. § 229F(1)(A). The phrase “purpose not prohibited under this chapter,” is then defined, in part, as “[a]ny peaceful purpose related to an industrial, agricultural, research, medical, or pharmaceutical activity or other activity.” Id. § 229F(7)(A). It is that “peaceful purpose” language that Bond urges us to take as our interpretive lodestar.

Specifically, Bond argues that, by looking to the “peaceful purpose” exception, we can employ a “common sense interpretation of § 229” that avoids “mak[ing] every malicious use of a household chemical”—including her own—a federal offense. (Appellant’s Supp. Br. at 17.) All we need do is “interpret the statute ... to reach [only the kind of acts] that would violate the Convention if undertaken by a signatory state.” (Id. at 14.) In other words, as Bond sees it, the modifier “peaceful” should be understood in contradistinction to “warlike” (3d Cir. Argument at 23), and, when so understood, the statute will not reach “conduct that no signatory state could possibly engage in—such as using chemicals in an effort to poison a romantic rival,” as Bond did. (Appellant’s Supp. Br. at 40.) That interpretation is tempting, in light of the challenges inherent in the Act’s remarkably broad language, but, as we held first time we had this case, Bond’s behavior “clearly constituted unlawful possession and use of a chemical weapon under § 229.” Bond I, 581 F.3d at 139.

That holding is in better keeping with the Act’s use of the term “peaceful purpose” than the construction Bond would have us give it. The ordinary meaning of “peaceful” is “untroubled by conflict, agitation, or commotion,” “of or relating to a state or time of peace,” or “devoid of violence or force,” Merriam-Webster’s Collegiate Dictionary 852 (10th ed. 2002), and Bond’s “deploy[ment] of highly toxic chemicals with the intent of harming Haynes,” Bond I, 581 F.3d at 139, can hardly be characterized as “peaceful” under that word’s commonly understood meaning; cf. Jones v. United States, 529 U.S. 848, 857–58, 120 S.Ct. 1904, 146 L.Ed.2d 902 (2000) (interpreting the federal arson statute not to reach “traditionally local criminal conduct” since the statute was “susceptible of two constructions” (citation and internal quotation marks omitted)). The term “peaceful,” moreover, does not appear in isolation: the Act only excludes from its ambit “peaceful purpose[s] ... related to

7. The Act’s breadth is certainly striking, seeing as it turns each kitchen cupboard and cleaning cabinet in America into a potential chemical weapons cache. Cf. Transcript of Oral Argument at 29, Bond v. United States, — U.S. —, 131 S.Ct. 2355, 180 L.Ed.2d 269 (2011) (Justice Alito’s statement during oral argument that “pouring a bottle of vinegar in [a] friend’s goldfish bowl” could constitute the use of a chemical weapon under the Act and expose a person to years in federal prison). We observed as much the last time this case was before us, noting, as Bond had herself acknowledged at the time, that the Act’s wide net was cast “for obvious reasons.” Bond I, 581 F.3d at 139. Ultimately, however, we concluded that the Act was not unconstitutionally overbroad. See id. (observing that the Act is “certainly broad,” but not unconstitutionally so). Bond did not challenge that determination, see Petition for Writ of Certiorari, Bond v. United States (No. 09–1227), 2010 WL 1506717 at *1, and it remains undisturbed. That the Act is not unconstitutionally overbroad, of course, does not preclude Bond from arguing as she now does, that the Act offends the Constitution’s division of power between the federal government and the states to the extent it is used to make her conduct a federal crime.
an industrial, agricultural, research, medical, or pharmaceutical activity or other activity.” 18 U.S.C. § 229F(7)(A) (emphasis added). Bond’s attacks on Haynes—even if non-warlike—were certainly not “related to an industrial, agricultural, research, medical, or pharmaceutical activity.” Id. Nor can her use of chemicals be said to be a “peaceful purpose[ ] ... related to an ... other activity,” because regarding her assaultive behavior as such would improperly expand § 229F(7)(A)’s scope. See, e.g., Gooch v. United States, 297 U.S. 124, 129, 56 S.Ct. 395, 80 L.Ed. 522 (1936) (“The rule of ejusdem generis ... [ordinarily ... limits general terms which follow specific ones to matters similar to those specified.”).

Thus, while one may well question whether Congress envisioned the Act being applied in a case like this, the language itself does cover Bond’s criminal conduct. And, given the clarity of the statute, we cannot avoid the constitutional question presented. See United States v. Stevens, — U.S. ——, 130 S.Ct. 1577, 1591, 176 L.Ed.2d 435 (2010) (stating that only “ambiguous statutory language [should] be construed to avoid serious constitutional doubts’” (alteration in original) (citation omitted)); United States v. Locke, 471 U.S. 84, 96, 105 S.Ct. 1785, 85 L.Ed.2d 64 (1985) (“We cannot press statutory construction ‘to the point of disingenuous evasion’ even to avoid a constitutional question.” (quoting George Moore Ice Cream Co. v. Rose, 289 U.S. 373, 379, 53 S.Ct. 620, 77 L.Ed. 1265 (1933))). It is not our prerogative to rewrite a statute, and we see no sound basis on which we can accept Bond’s construction of the Act without usurping Congress’s legislative role. Though we agree it would be better, if possible, to apply a limiting construction to the Act rather than consider Bond’s argument that it is unconstitutional, see Burton v. United States, 196 U.S. 283, 295, 25 S.Ct. 243, 49 L.Ed. 482 (1905) (“It is not the habit of the court to decide questions of a constitutional nature unless absolutely necessary to a decision of the case”), the statute speaks with sufficient certainty that we feel compelled to consider the hard question presented in this appeal.

B. Constitutionality of the Act as Applied

Understanding whether application of the Act to Bond violates the structural limits of federalism begins with the Tenth Amendment, which Bond cites and which provides that “[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.” U.S. Const. amend. X. That text, as the Supreme Court has observed, “confirms that the power of the Federal Government is subject to limits that may ... reserve power to the States.” New York v. United States, 555 U.S. 144, 157, 112 S.Ct. 2408, 120 L.Ed.2d 129 (1992). Thus, it encapsulates the principles of federalism upon which our nation was founded. See D.A. Jeremy Telman, A Truism That Isn’t True? The Tenth Amendment and Executive War Power, 51 Cath. U.L.Rev. 135, 143-44 (2001) (describing the argument that “the Tenth Amendment has a declaratory function and provides a rule of constitutional interpretation rather than a rule of constitutional law”).

8. We do not need to determine whether the Tenth Amendment is a tautology reflecting the structural limitations on federal power embodied in the system of dual sovereignty established by the Constitution, or, as has sometimes been suggested, serves as an independent check on federal power. See New York, 555 U.S. at 156, 159, 112 S.Ct. 2408 (describing the argument that, even when Congress has the authority to regulate, “the
Endeavoring to discover what impact the Tenth Amendment may have on treaty-implementing legislation immediately leads, as we have indicated, to the Supreme Court’s decision in Missourri v. Holland. The statute at issue in that case, the Migratory Bird Treaty Act, 16 U.S.C. § 708, implemented a treaty between the United States and Great Britain that banned the hunting of migratory birds during certain seasons. Holland, 252 U.S. at 431, 40 S.Ct. 382. The State of Missouri brought suit against a U.S. game warden, arguing that the statute unconstitutionally interfered with the rights reserved to Missouri by the Tenth Amendment because Missouri was free to do what it wished with the birds while they were within its borders. Id. at 431–32, 40 S.Ct. 382. The Supreme Court, speaking through Justice Holmes, rejected that argument, reasoning that “it is not enough to refer to the Tenth Amendment, reserving the powers not delegated to the United States, because by Article 2, Section 2, the power to make treaties is delegated expressly.” Id. at 432, 40 S.Ct. 382.

As noted earlier, the Court made it clear that Congress may, under the Necessary and Proper Clause, legislate to implement a valid treaty, regardless of whether Congress would otherwise have the power to act or whether the legislation causes an intrusion into what would otherwise be within the state’s traditional province. Id. at 432–33, 40 S.Ct. 382. While the Court did allow that there may be “qualifications to the treaty-making power,” it also said, somewhat obscurely, that they had to be found “in a different way” than one might find limitations on other grants of power to the federal government. Id. at 433, 40 S.Ct. 382. After implying that Congress’s powers are particularly sweeping when dealing with “matters requiring national action,” the Court suggested one limitation on the Treaty Power: if the implementation of a treaty “contraven[e] any prohibitory words to be found in the Constitution,” then it may be unconstitutional. Id. (citation omitted). Since the treaty in question did not do that, the only remaining question was “whether it [was] forbidden by some invisible radiation from the general terms of the Tenth Amendment.” Id. at 433–34, 40 S.Ct. 382. The Court concluded that it was not. See id. (reasoning that, while “the great body of private relations usually fall within the control of the State, ... a treaty may override its power”). Finally, the Court assumed with-

Tenth Amendment limits the power of Congress to regulate in the way it has chosen,” though noting that its actual limit is “not derived from the text” of the Tenth Amendment as the Tenth Amendment is “essentially a tautology”; Nat’l League of Cities v. Usery, 426 U.S. 833, 842, 96 S.Ct. 2465, 49 L.Ed.2d 245 (1976) (recognizing a “limit[.] upon the power of Congress to override state sovereignty, even when exercising its otherwise plenary powers ... which are conferred by Art. I of the Constitution” and that “an express declaration of this limitation is found in the Tenth Amendment”), overruled by Garcia v. San Antonio Metro. Transit Auth., 469 U.S. 528, 105 S.Ct. 1005, 83 L.Ed.2d 1016 (1985); cf. Gerard N. Magliocca, A New Approach to Congressional Power: Revisiting the Legal Tender Cases, 95 Geo. L.J. 119, 125 n. 30 (2006) (suggesting the Tenth Amendment’s “independent force” is limited to “[l]aws that regulate states qua states”). Regardless of whether the Tenth Amendment has “independent force of its own,” Bond II, 131 S.Ct. at 2367, we understand our constitutional inquiry to turn on whether principles of federalism are violated by the Act, in light of the Constitution’s delegation to the President of the power “to make Treaties, provided two thirds of the Senators present concur,” U.S. Const. art. II, § 2, cl. 2, and to Congress of the power to enact “all Laws which shall be necessary and proper for carrying into Execution ... all other Powers vested by the Constitution in the Government of the United States, or in any Department or Officer thereof,” U.S. Const. art. I, § 8, cl. 18.
out further discussion that, because the treaty was valid, so was the implementing statute. See id. at 435, 40 S.Ct. 382 ("We see nothing in the Constitution that compels the Government to sit by while a food supply is cut off and the protectors of our forests and our crops are destroyed.").

[2,3] In sum, Holland teaches that, when there is a valid treaty, Congress has authority to enact implementing legislation under the Necessary and Proper Clause, even if it might otherwise lack the ability to legislate in the domain in question.9 See United States v. Lara, 541 U.S. 193, 201, 124 S.Ct. 1628, 158 L.Ed.2d 420 (2004) ("[A]s Justice Holmes pointed out [in Holland], treaties made pursuant to [the Treaty Power] can authorize Congress to deal with 'matters' with which otherwise 'Congress could not deal.' ") (quoting Holland, 252 U.S. at 435, 40 S.Ct. 382)). The legislation must, of course, meet the Necessary and Proper Clause's general requirement that legislation implemented under that Clause be "rationally related to the implementation of a constitutionally enumerated power." United States v. Comstock, — U.S. —, 130 S.Ct. 1949, 1956, 176 L.Ed.2d 878 (2010); see also McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 421, 4 L.Ed. 579 (1819) ("[A]ll means which are appropriate, which are plainly adapted to that end, which are not prohibited, but consist with the letter and spirit of the constitution, are constitution- al."). In the treaty context, that requirement has been understood to mean that a treaty and its implementing legislation must be rationally related to one another. United States v. Ferreira, 275 F.3d 1020, 1027 (11th Cir.2001). Thus, as long as "the effectuating legislation bear[s] a rational relationship to" a valid treaty, United States v. Lu, 134 F.3d 79, 84 (2d Cir.1998), the arguable consequence of Holland is that treaties and associated legislation are simply not subject to Tenth Amendment scrutiny, no matter how far into the realm of states' rights the President and Congress may choose to venture. See Curtis A. Bradley, The Treaty Power and American Federalism, 97 Mich. L.Rev. 390, 395 (1998) (taking exception with Holland to the extent it can be read to say that "the treaty power is immune from federalism restrictions because that power has been exclusively delegated to the federal government"); Erwin Chemerinsky, Constitutional Law Principles and Policies 287 (4th ed. 2011) (stating that the Holland court "rejected the claim that state sovereignty and the Tenth Amendment limit the scope of the treaty power"); Louis Henkin, Foreign Affairs and the U.S. Constitution 191 (2nd ed.

9. It has been argued that Holland incorrectly permits "treaties ... [to] expand the legislative power of Congress." Nicholas Quinn Rosenkranz, Executing The Treaty Power, 118 Harv. L.Rev. 1867, 1875 (2005). The Cato Institute has submitted an amicus brief taking that position, arguing against Holland's "implication" that if a treaty commits the United States to enact some legislation, then Congress automatically obtains the power to enact that legislation, even if it would lack such power in the absence of the treaty. (Amicus Br. at 6.) Amicus argues that Congress's authority to act in connection with the Treaty Power only permits it to enact those laws that are necessary and proper to permit the President to make treaties—not to implement treaties once they are agreed upon. (See id. (arguing the President cannot increase Congress's power under the Necessary and Proper Clause by entering into a treaty).) Under that view, Congress could, for example, legislate to provide funding for an office of treaty-making, but could not have implemented the broadly worded Convention involved here. (See id. at 8 ("[T]his power would ... embrace any ... laws necessary and proper to ensuring the wise use of the power to enter treaties.").) Holland remains binding precedent, however, and forecloses this line of reasoning.
clear that the Tenth Amendment should not be treated as irrelevant when examining the validity of treaty-implementing legislation. (See Appellant's Supp. Br. at 24 (“[I]n recent decades, the Supreme Court has reasserted the critical role of the Tenth Amendment in preserving the proper balance of authority between federal and state government to ensure that all levels of government represent and remain accountable to the People.”)). Concluding otherwise, she asserts, would make “nothing . . . off-limits” in a world where, more and more, “international treaties govern[ ] a virtually unlimited range of subjects and intrud[e] deeply on internal concerns.” (See id. at 20.) That latter point is not without merit. Juxtaposed against increasingly broad conceptions of the Treaty Power’s scope, reading Holland to confer on Congress an unfettered ability to effectuate what would now be considered by some to be valid exercises of the Treaty Power runs a significant risk of disrupting the delicate balance between state and federal authority.10

10. The Supreme Court has focused renewed attention on federalism over the last two decades. Although many earlier cases reflect the importance of the our Constitution’s basic provision for dual sovereigns, see, e.g., Gregory v. Ashcroft, 501 U.S. 452, 460, 111 S.Ct. 2395, 115 L.Ed.2d 410 (1991) (observing that the rule requiring Congress to speak clearly in order to preempt state law “acknowledges[ ] that the States retain substantial sovereign powers under our constitutional scheme”); South Dakota v. Dole, 483 U.S. 203, 211–12, 107 S.Ct. 2793, 97 L.Ed.2d 171 (1987) (recognizing that Congress may not coerce the states when exercising its power to spend), more recent cases have been particularly pointed in describing the role federalism principles should play in analyzing assertions of federal authority. That trend began at least as early as the Court’s decision in New York v. United States, 505 U.S. 144, 112 S.Ct. 2408, 120 L.Ed.2d 120 (1992), which held that the federal government could not “commandeer[ ] the legislative processes of the States.” Id. at 176, 112 S.Ct. 2408 (citation and internal quotation marks omitted). After New York, the Court struck down legislation criminalizing local conduct in United States v. Lopez, 514 U.S. 549, 115 S.Ct. 1624, 131 L.Ed.2d 626 (1995), as beyond the Commerce Clause Power. In doing so the Court recognized the importance of the states’ authority to “define[e] and enforc[e] the criminal law,” and noted that, “[w]hen Congress criminalizes conduct already denounced as criminal by the States, it effects a change in the sensitive relation between federal and state criminal jurisdiction.” Id. at 561 n. 3, 115 S.Ct. 1624 (citations and internal quotation marks omitted). In Printz v. United States, 521 U.S. 898, 919, 117 S.Ct. 2365, 138 L.Ed.2d 914 (1997), the Court likewise considered principles of federalism in striking down legislation that required state police to perform background checks on potential gun owners. See id. at 919, 117 S.Ct. 2365 (noting the establishment of dual sovereignties was “reflected throughout the Constitution’s text,” and had vested in the states “a residuary and inviola-
Those concerns notwithstanding, Bond does not argue that the Convention itself is constitutionally infirm. On the contrary, she admits “that a treaty restricting chemical weapons is a ‘proper subject[ ] of negotiations between our government and other nations.’” (Id. at 4–5 (alteration in original) (citation omitted)). Accordingly, we need not tackle, head on, whether an arguably invalid treaty has led to legislation encroaching on matters traditionally left to the police powers of the states. Nevertheless, resolving the argument Bond does lodge against her prosecution requires at least some consideration of whether the Convention is, in fact, valid. See Holland, 252 U.S. at 432, 40 S.Ct. 382 (“If the treaty is valid there can be no dispute about the validity of the statute . . . .” (emphasis added)). We therefore turn briefly to whether the Convention falls within the Treaty Power’s appropriate scope, bearing in mind that Bond seems to accept that it does.

1. The Convention’s Validity

The Constitution does not have within it any explicit subject matter limitation on the power granted in Article II, § 2. That section states simply that the President has the “Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur.” U.S. Const. art. II, § 2, cl. 2. Throughout much of American history, however, including when Holland was handed down, it was understood that the Treaty Power was implicitly limited to certain subject matters. See Bradley, supra, at 429 (arguing that “a subject matter limitation [on the Treaty Power] appears to have been assumed both during the Founding and at times during the nineteenth century,” and suggesting it was likewise assumed by the Holland court); Golove, supra, at 1288 (“[V]irtually every authority, including the Supreme Court, has on countless occasions from the earliest days recognized general subject matter limitations on treaties.”).

Contemporaneous records such as the Virginia Ratifying Convention show that the Founders generally accepted that the purpose of treaties was, as James Madison put it, to regulate “intercourse with foreign nations,” and that the “exercise” of the Treaty Power was expected to be “consistent with” those “external” ends.\footnote{Other Founders shared Madison’s understanding that the Treaty Power would be limited to matters involving foreign affairs. Cf. The Federalist No. 64 (John Jay) (noting that the “power of making treaties is an important one, especially as it relates to war, peace, and commerce”); The Federalist No. 75 (Alexander Hamilton) (stating that treaties “[were] not rules prescribed by the sovereign to the subject, but agreements between sovereign and sovereign”). Notwithstanding the Founders’ view of the Treaty Power’s inherent limits, there is, again, nothing in the Constitution’s text explicitly confining that power. The basis for that omission is perhaps best explained by Madison, who, like others, recognized the need for flexibility with respect to the Treaty Power and cautioned against expressly defining its scope:}

I do not think it possible to enumerate all the cases in which such external regulations would be necessary. Would it be right to define all the cases in which Congress could exercise this authority? The definition might, and probably would, be defective.
The Debates in The Several State Conventions on the Adoption of the Constitution 514–15 (Jonathan Elliot ed., 2d ed. 1941) ("The Virginia Debates"); see The Federalist No. 45 (James Madison) (stating that the Treaty Power "will be exercised principally on external objects, as war, peace, negotiation, and foreign commerce"). As Madison later explained, if there was no limitation on the Treaty-making power . . ., it might admit of a doubt whether the United States might not be enabled to do those things by Treaty which are forbidden to be done by Congress . . .; but no such consequence can follow, for it is a sound rule of construction, that what is forbidden to be done by all the branches of Government conjointly, cannot be done by one or more of them separately.

5 Annals of Congress 671 (1796) (emphasis added).

Early cases followed that reasoning and indicated that the Treaty Power is confined to matters traditionally understood to be of international concern. See, e.g., Ross v. McIntyre, 140 U.S. 453, 463, 11 S.Ct. 897, 35 L.Ed. 581 (1891) ("The treaty-making power vested in our government extends to all proper subjects of negotiation with foreign governments."); De Geofroy v. Riggs, 133 U.S. 258, 266, 10 S.Ct. 295, 33 L.Ed. 642 (1890) ("That the treaty power of the United States extends to all proper subjects of negotiation between our government and the governments of other nations is clear."); Holden v. Joy, 84 U.S. (17 Wall.) 211, 243, 21 L.Ed. 523 (1872) ("[W]e assume the power is given, in general terms, without any description of the objects intended to be embraced within its scope, it must be assumed that the

They might be restrained, by such a definition, from exercising the authority where it would be essential to the interest and safety of the community. It is most safe, therefore, to leave it to be exercised as contingencies may arise.

The Virginia Debates, supra, at 514–15.
jects of negotiation between our government and other nations.”), and that the purpose of limiting the Treaty Power to matters which “in the ordinary intercourse of nations had usually been made subjects of negotiation and treaty” was to ensure that treaties were “consistent with . . . the distribution of powers between the general and state governments,” Holmes v. Jennison, 39 U.S. (14 Pet.) 540, 569, 10 L.Ed. 579 (1840).

Despite the long history of that view of the Treaty Power, the tide of opinion, at least in some quarters, has shifted decisively in the last half-century. Many influential voices now urge that there is no limitation on the Treaty Power, at least not in the way understood from the founding through to the middle of the Twentieth Century. See Bradley, supra, at 433 (describing the “rejection of a subject matter limitation on the treaty power” as “the accepted view”). That change is reflected in the Restatement (Third) of Foreign Relations Law of the United States (1987) (the “Third Restatement”), which declares flatly that, “[c]ontrary to what was once suggested, the Constitution does not require that an international agreement deal only with ‘matters of international concern.’” Third Restatement § 302 cmt. c; see id. § 303(1) (“[T]he President, with the advice and consent of the Senate, may make any international agreement of the United States in the form of a treaty.”).

Whatever the Treaty Power’s proper bounds may be, however, we are confident that the Convention we are dealing with here falls comfortably within them. The Convention, after all, regulates the proliferation and use of chemical weapons. One

12. Although at least one commentator has disputed that shift, see Golove, supra, at 1281, 1289 (stating that “[c]ommentators . . . have not rejected subject matter limitations” to the treaty power and arguing that, “[w]here the President and Senate to make a treaty on a subject inappropriate for negotiation and agreement, and thus beyond the scope of the treaty power, the treaty would be invalid under the Tenth Amendment”), even then it has been acknowledged that “the traditional subject matter limitations on treaties are very general, and with globalization, the matters appropriate for treaties have expanded and will continue to do so,” id. at 1291. That reality has been borne out by the kinds of conventions now extant in the international community. See Bradley, supra, at 397 n. 29 (citing to, inter alia, the Convention on the Rights of the Child, open for signature Nov. 20, 1989, 28 I.L.M. 1456 (1989); the Convention on the Elimination of All Forms of Discrimination Against Women, S. Exec. Rep. No. 103–38 (1994); and the International Covenant on Economic, Social, and Cultural Rights, open for signature Dec. 19, 1966, 6 I.L.M. 360 (1967)). Considering the expanding subjects taken up in treaty-making and the nebulous standards associated with any lingering subject matter limitation, see Golove, supra, at 1090 (“The implication is clear: the President and Senate can make treaties on any subject appropriate for negotiation and agreement among states.” (emphasis added)); Laurence H. Tribe, Taking Text and Structure Seriously: Reflections on Free-Form Method in Constitutional Interpretation, 108 Harv. L.Rev. 1221, 1261 n. 133 (1995) (“The Treaty Power is legitimate only for international agreements fairly related to foreign relations” (emphasis added)), whether the subject matter limitation has fully eroded is a serious question. For now, however, it is enough to note that, at least among certain commentators, it is no longer viewed as a meaningful restraint on the Treaty Power. Cf. Henkin, supra, at 197 & n. 89 (citing the Third Restatement for the proposition that a limitation on the Treaty Power to matters of international concern “has now been authoritatively abandoned”).

13. It, evidently, is not alone in that view. See, e.g., Tribe, supra, at 1261 n. 133 (“[E]stablishment of a joint, binational health care system by a treaty followed by implementing legislation would presumably be possible . . . .”); Henkin, supra, at 474 (“[W]hat is essentially a matter of ‘domestic concern’ becomes a matter of ‘international concern’ if nations do, in fact, decide to bargain about it.”).
need not be a student of modern warfare to have some appreciation for the devastation chemical weapons can cause and the corresponding impetus for international collaboration to take steps against their use. Given its quintessentially international character, we conclude that the Convention is valid under any reasonable conception of the Treaty Power's scope. In fact, as we discuss at greater length herein, because the Convention relates to war, peace, and perhaps commerce, it fits at the core of the Treaty Power. See infra note 18.

2. Interpreting Holland

Because Holland clearly instructs that "there can be no dispute about the validity of [a] statute" that implements a valid treaty, 252 U.S. at 432, 40 S.Ct. 382, the constitutionality of Bond's prosecution would seem to turn on whether the Act goes beyond what is necessary and proper to carry the Convention into effect, or, in other words, whether the Act fails to "bear a rational relationship to" the Convention, Lue, 134 F.3d at 84. According to Bond, however, only a simplistic reading of Holland could lead one to think that the Supreme Court was saying that "Congress's power to implement treaties is subject to no limit other than affirmative restrictions on government power like the First Amendment." (Appellant's Supp. Reply Br. at 9-10.)

The problem with Bond's attack is that, with practically no qualifying language in Holland to turn to, we are bound to take at face value the Supreme Court's statement that "[i]f the treaty is valid there can be no dispute about the validity of the statute ... as a necessary and proper means to execute the powers of the Government." 252 U.S. at 432, 40 S.Ct. 382. A plurality of the Supreme Court itself apparently gave that passage the simplistic reading Bond denounces when it said, in Reid v. Covert, 354 U.S. 1, 77 S.Ct. 1222, 1 L.Ed.2d 1148 (1957), that:

The Court [in Holland] was concerned with the Tenth Amendment which reserves to the States or the people all power not delegated to the National Government. To the extent that the United States can validly make treaties, the people and the States have delegated their power to the National Government and the Tenth Amendment is no barrier.

Id. at 18, 77 S.Ct. 1222.

It is true that Justice Holmes spoke later in Holland in language that implies a balancing of the national interest against the interest claimed by the State, see Holland, 252 U.S. at 435, 40 S.Ct. 382 ("Here a national interest of very nearly the first magnitude is involved."). But that was in the context of assessing the validity of the Migratory Bird Treaty itself, not the implementing statute. That the latter was constitutional in light of the validity of the former seemed to the Supreme Court to require no further comment at all.15

14. Because we conclude that the Act is valid under the Necessary and Proper Clause, we express no opinion as to the merits of the Government's newly-discovered Commerce Clause argument.

15. Bond recognizes that the Holland court "treated the legislation and treaty as co-extensive." (Appellant's Supp. Br. at 23.) Her conclusion from that is that when a treaty and its implementing legislation are not coextensive, the justification for enacting the legislation under the Necessary and Proper clause can collapse. We do not disagree; as noted, a treaty and treaty-implementing legislation must be "rationally related." Ferreira, 275 F.3d at 1027. As we discuss at greater length infra, however, the Act and the Convention with which we are dealing here are coextensive at least on the question of "use," which is the only point relevant to Bond's-as-applied challenge. See infra Part II.B.3.
That does not mean, of course, that the Holland court would have spoken in the same unqualified terms had it foreseen the late Twentieth Century's changing claims about the limits of the Treaty Power, or had it been faced with a treaty that transgressed the traditional subject matter limitation. See id. at 433, 40 S.Ct. 382 ("The case before us must be considered in light of our whole experience and not merely in that of what was said a hundred years ago."). It may well have chosen to say more about how to assess the validity of a treaty, and hence of coextensive treaty-implementing legislation. Perhaps Holland's vague comment about "invisible radiation[s] from the general terms of the Tenth Amendment," id. at 434, 40 S.Ct. 382, would have been given some further explication. As we have previously described, when Holland was decided, and, more importantly, when the Founders created the Treaty Power, it was generally understood that treaties should concern only matters that were clearly "international" in character, matters which, in Holland's words, invoke a national interest that "can be protected only by national action in concert with that of another [sovereign nation]." Id. at 435, 40 S.Ct. 382. All the authors of The Federalist Papers, along with others from that era, considered the Treaty Power to be a necessary attribute of the central government for the important but limited purpose of permitting our "intercourse with foreign nations," The Virginia Debates, supra, at 514 (statement of James Madison), and thereby allowing for compacts "especially as [they] relate[] to war, peace, and commerce," The Federalist No. 64 (John Jay); see supra Part II.B.1. It was not a general and unlimited grant of power to the federal government.

Because an implied subject matter limitation on the Treaty Power was a given at the time Holland was written, it was enough to answer the states' rights question in that case by pointing out that the Tenth Amendment only reserves those powers that are not delegated and that "the power to make treaties is delegated expressly." 252 U.S. at 432, 40 S.Ct. 382. Thus, Holland's statement that "there can be no dispute about the validity" of a statute implementing a valid treaty, id., is

16. The treaty at issue in Holland involved a subject of traditional international concern. See 56 Cong. Rec. 7361 (1918) (legislative testimony that the Migratory Bird Treaty Act "is essential to the preservation of our cotton, grain, and timber crops, whilst the migratory game birds contribute materially to our food supply. The bill may well be considered a measure of importance as affecting the successful prosecution of the war in which we are now engaged"). As the Holland court noted, "nothing in the Constitution ... compelle[d] the Government to sit by while a food supply [was] cut off and the protectors of our forests and our crops [were] destroyed." 252 U.S. at 435, 40 S.Ct. 382. Consequently, the treaty dealt with "a national interest of very nearly the first magnitude" that could "only [be furthered] by national action in concert with that of another power." Id. at 435, 40 S.Ct. 382; see id. at 433, 40 S.Ct. 382 (stating that the treaty dealt with a "matter[] of the sharpest exigency" and that "the States individually [were] incompetent to act").

17. That the Founders understood Article II, § 2 to be a limited grant of power is clear, as the Tenth Amendment itself verifies. The available evidence of their thinking is that they did not intend for treaties to become a vehicle to usurp the general powers reserved to the states. Cf. United States v. Pink, 315 U.S. 203, 230, 62 S.Ct. 552, 86 L.Ed. 796 (1942) ("It is of course true that even treaties with foreign nations will be carefully construed so as not to derogate from the authority and jurisdiction of the States of this nation unless clearly necessary to effectuate the national policy."); Holmes, 39 U.S. at 569, 39 U.S. 540 ("The power to make treaties ... was designed to [be] ... consistent with ... the distribution of powers between the general and state governments.").
We pause to consider how, if *Holland* were not so clear in its "valid treaty equal valid implementing legislation" holding, treaties and implementing legislation might usefully be reviewed in light of the apparently evolving understanding of the Treaty Power that we have described. *See supra* Part II.B.1. The Founders deliberately drafted Article II, § 2 without defining the limits of the Treaty Power because they decided its scope required flexibility in the face of unknowable future events. *Cf. The Virginia Debates, supra,* at 514–15 (James Madison’s observation that “it is not possible to enumerate all the cases in which such external regulations would be necessary…. It is most safe, therefore, to leave it to be exercised as contingencies may arise”). We do not second guess the wisdom of their choice and acknowledge that any attempt to precisely define a subject matter limitation on the Treaty Power would involve political judgments beyond our ken. *Cf. Baker v. Carr,* 369 U.S. 186, 211, 82 S.Ct. 691, 7 L.Ed.2d 663 (1962) (stating that resolution of issues “touching foreign relations” often "turn on standards that defy judicial application, or involve the exercise of a discretion demonstrably committed to” a coordinate branch); *Pink,* 315 U.S. at 232, 62 S.Ct. 552 ("[T]he field which affects international relations is 'the one aspect of our government that from the first has been most generally conceded imperatively to demand broad national authority'…. " (citation omitted)); *Lua,* 134 F.3d at 83 ("[I]t is not the province of the judiciary to impinge upon the Executive's prerogative in matters pertaining to foreign affairs.").

Nevertheless, while the outer boundaries of the Treaty Power may be hard to delineate, we can safely say that certain kinds of treaties fall within the core of that power, namely those dealing with war, peace, foreign commerce, and diplomacy directed to those ends. *See The Federalist No. 45* (James Madison) (stating that the Treaty Power "will be exercised principally on external objects, as war, peace, negotiation, and foreign commerce"); *The Federalist No. 64* (John Jay) (stating the "power of making treaties is an important one, especially as it relates to war, peace, and commerce"). As to treaties of such character, it is hard to argue with the reasoning in *Holland* that, because "the power to make treaties is delegated expressly," 252 U.S. at 432, 40 S.Ct. 382, the Tenth Amendment has nothing meaningful to say. However, just as some treaties may fall comfortably within the traditionally understood bounds of the Treaty Power, some may be negotiated that will plainly fall outside that scope. If such a treaty were challenged, a court would be bound to take up an issue not present here, namely whether and when a treaty has reached a constitutional boundary, *see Marbury v. Madison,* 5 U.S. (1 Cranch) 137, 177, 2 L.Ed. 60 (1803) ("It is emphatically the province and duty of the judicial department to say what the law is."); *cf. Baker,* 369 U.S. at 211, 82 S.Ct. 691 (observing that not "every case or controversy which touches foreign relations lies beyond judicial cognizance"), recognizing that a treaty falling outside the limits of the Treaty Power would be unconstitutional as ultra vires, *cf. Joseph Story,* *Commentaries on the Constitution of the United States* 339 (Melville M. Bigelow, ed. 5th ed. 1994) (1891) ("A treaty to change the organization of the government, or annihilate its sovereignty, to overturn its republican form, or to deprive it of its constitutional powers, would be void."). The deliberately vague boundaries of the Treaty Power would probably relegate that court to the unenviable position of saying it knew a violation when it saw one.

Before the outer limits of the treaty power are reached, however, it may be that federalism does have some effect on a treaty’s constitutionality. While it is no: our prerogative to ignore *Holland*’s rejection of federalism limitations upon the Treaty Power, the Supreme Court could clarify whether principles of federalism have any role in assessing an exercise of the Treaty Power that goes beyond the traditionally understood subject matter for treaties. *Holland* itself indicates that "invisible radiation[s] from the general terms of the Tenth Amendment" may be pertinent in deciding whether there is any space between obviously valid treaties and obviously ultra vires treaties and whether, in that space, some judicial review of treaties and their im-
demands from us a direct acknowledgement of its meaning, even if the result may be viewed as simplistic. If there is nuance there that has escaped us, it is for the Supreme Court to elucidate.

3. The Necessary and Proper Clause

[4] Thus, because the Convention falls comfortably within the Treaty Power's traditional subject matter limitation, the Act is within the constitutional powers of the federal government under the Necessary and Proper Clause and the Treaty Power, unless it somehow goes beyond the Convention. Bond argues that it does.19

She says that the Act covers a range of activity not actually banned by the Convention and thus cannot be sustained by the Necessary and Proper Clause. Whether that argument amounts to a facial or an as-applied attack on the Act, see supra note 5, it fails. We stated in Bond I that “Section 229 . . . closely adheres to the language of the . . . Convention,” 581 F.3d at 138, and so it does. True, as Bond notes, the Convention bans persons from using, developing, acquiring, stockpiling, or retaining chemical weapons, 32 I.L.M. at 804, while the Act makes it unlawful to “receive, stockpile, retain, own, possess, use, or threaten to use” a chemical weapon, 18 U.S.C. § 229(a)(1), but those differences in wording do not prove that the Act has materially expanded on the Convention. See United States v. Belfast, 611 F.3d 783, 806 (11th Cir.2010) (“[T]he existence of slight variances between a treaty and its congressional implementing legislation do not make the enactment unconstitutional; identity is not required.”).

The meaning of the list in the former seems rather to fairly encompass the latter (with the possible exception of the “threaten to use” provision of the Act) and, if the Act goes beyond the Convention at all, does not do so in the “use” aspect at issue here.

So while Bond's prosecution seems a questionable exercise of prosecutorial discretion,20 and indeed appears to justify her assertion that this case “trivializes the concept of chemical weapons” (Appellant's Supp. Br. at 53), the treaty that gave rise to it was implemented by sufficiently related legislation. See Comstock, 130 S.Ct. at 1956 (“[I]n determining whether the Necessary and Proper Clause grants Congress the legislative authority to enact a particular federal statute, we look to see whether the statute constitutes a means that is rationally related to the implementation of a constitutionally enumerated power.”);

Lue, 134 F.3d at 84 (rejecting the argument “that because the Hostage Taking Convention targets a specific aspect of international terrorism—hostage taking—the statute effectuating the Convention must deal narrowly with international terrorism or risk invalidity” as a “cramped”

implementing legislation may be undertaken to preserve the federal structure of our government. The “invisible radiation[s]” imagery, 252 U.S. at 433–34, 40 S.Ct. 382, is unusual but, in light of current conceptions about the breadth of the Treaty Power, it may well be worth taking seriously. Cf. Printz, 521 U.S. at 921–22, 117 S.Ct. 2365 (stating that the concept of dual sovereignty was "one of the Constitution's structural protections of liberty").

19. As Judge Rendell correctly points out in her concurrence, Bond’s emphasis is entirely misplaced to the extent she may be contending that her prosecution violates the Necessary and Proper Clause because the United States did not have to prosecute her to comply with its obligations under the Convention. (See Rendell Concurrence Op. at 167 (“Examining the scope of Congress’s Necessary and Proper Power by definition requires us to examine the Act, not its enforcement.”).)

20. The decision to use the Act—a statute designed to implement a chemical weapons treaty—to deal with a jilted spouse’s revenge on her rival is, to be polite, a puzzling use of the federal government’s power.
view of Congressional authority, because treaty-implementing legislation must simply "bear a rational relationship to a permissible constitutional end").

In short, because the Convention pertains to the proliferation and use of chemical weapons, which are matters plainly relating to war and peace, we think it clear that the Convention falls within the Treaty Power's core. See supra note 18. Consequently, we cannot say that the Act disrupts the balance of power between the federal government and the states, regardless of how it has been applied here. See Gonzales v. Raich, 545 U.S. 1, 23, 125 S.Ct. 2195, 162 L.Ed.2d 1 (2005) ("[W]here the class of activities is regulated and that class is within the reach of federal power, the courts have no power to excise, as trivial, individual instances of the class." (citations and internal quotation marks omitted)); 21 Holland, 252 U.S. at 432, 40 S.Ct. 382 ("If the treaty is valid there can be no dispute about the validity of the [implementing] statute."); cf. U.S. Const. art. VI, cl. 2 ("[A]ll Treaties made ... shall be the supreme Law of the Land.").

III. Conclusion

For the foregoing reasons, we will affirm the judgment of conviction.

21. Although we acknowledge that the Raich court's admonition against excising a class of activities from a valid assertion of federal power may have related to its status as a Commerce Clause case based on the aggregation principle employed in that context, see Richard H. Fallon, Jr., Fact and Fiction About Facial Challenges, 99 Cal. L.Rev. 915, 936 (2011) (opining that Raich "can be read as rejecting the possibility of successful as-applied challenges to assertions of legislative power under the Commerce Clause"), the principle would seem to hold with respect to federalism challenges arising from treaties within the Treaty Power's core. As we have already observed, see supra note 18, it is hard to argue with Holland's rejection of federalism as an applicable concept as far as such treaties are concerned.

1. As her counsel argued:

And it really inheres in the statute. It's not that there's anything wrong in the abstract with the United States ratifying this treaty. That's not where the problem is.

The problem is either at the moment they passed the statute that necessarily went this far or at the point that it becomes applied in this kind of situation.

(3d Cir. Argument at 13.)
indeed, Ms. Bond unequivocally concedes that point. In turn, the Act, which implements the Convention, is valid as an exercise of Congress's Necessary and Proper Power. That is because the Necessary and Proper Clause affords Congress "ample means" to implement the Convention, and gives Congress the authority "to enact laws that are 'convenient, or useful' or 'conducive'... to the 'beneficial exercise'" of the federal government's Treaty Power. United States v. Comstock, — U.S. —, 130 S.Ct. 1949, 1956, 176 L.Ed.2d 878 (2010) (quoting McCulloch v. Maryland, 17 U.S. 316, 4 Wheat. 316, 408, 413, 418, 4 L.Ed. 579 (1819)). There is no question that the Act is rationally related to the Convention; it faithfully tracks the language of the Convention. Enacting a statute that essentially mirrors the terms of an underlying treaty is plainly a means which is "reasonably adapted to the attainment of a legitimate end"—ensuring that the United States complies with our international obligations under a valid treaty. Comstock, 130 S.Ct. at 1957 (internal quotation marks and citations omitted); see also United States v. Lue, 134 F.3d 79, 84 (2d Cir.1998) (upholding a statute implementing a treaty where "[t]he Act here plainly bears a rational relationship to the Convention; indeed, it tracks the language of the Convention in all material respects").

In examining the constitutionality of Congress's exercise of its Necessary and Proper Power, we need not consider whether the prosecution of Ms. Bond is necessary and proper to complying with the Convention, as she would have us do. In other words, she argues that no national-state would submit that the United States has failed to comply with its obligations under the Convention if the federal government did not prosecute Ms. Bond under the Act. But that is not the appropriate test. Examining the scope of Congress's Necessary and Proper Power by definition requires us to examine the Act, not its enforcement. To determine if the Act is necessary and proper, we ask whether it bears a rational relationship to the Convention. See Comstock, 130 S.Ct. at 1956 ("[I]n determining whether the Necessary and Proper Clause grants Congress the legislative authority to enact a particular federal statute, we look to see whether the statute constitutes a means that is rationally related to the implementation of a constitutionally enumerated power."). Ms. Bond's actions fall plainly within the terms of the Act, and the Act bears a rational relationship to the Convention. So ends the Necessary and Proper inquiry.

The foregoing conclusion is enough to affirm Ms. Bond's conviction. As the Majority correctly reasons, Missouri v. Holland, 252 U.S. 416, 40 S.Ct. 382, 64 L.Ed. 641 (1920), forecloses challenging a valid statute implementing a valid treaty on Necessary and Proper grounds or federalism grounds. See Maj. Op. at 163–65; Holland, 252 U.S. at 432, 40 S.Ct. 382 ("If the treaty is valid there can be no dispute about the validity of the statute" under the Necessary and Proper Clause).

But even if Ms. Bond were able to assert a federalism challenge to her conviction, she proposes no principle of federalism that would limit the federal government's authority to prosecute her under the Act. Thus, as to the second question, Ms. Bond argues that if the statute is applied to her, and, is thus read to "criminalize every malicious use of poisoning," then principles of federalism are violated by disturbing the division of power between the federal government and the states. (3d Cir. Argument at 15.) As appealing as the argument sounds—that a federal statute should not reach an essentially local offense like this—there is in fact no principled reason to limit the Act's reach when her conduct
is squarely prohibited by it. The fact that an otherwise constitutional federal statute might criminalize conduct considered to be local does not render that particular criminalization unconstitutional. As the Supreme Court explained in *Gonzales v. Raich*, when "the class of activities is regulated and that class is within the reach of federal power, the courts have no power to excise, as trivial, individual instances of the class." 545 U.S. 1, 23, 125 S.Ct. 2195, 162 L.Ed.2d 1 (2005) (internal quotation marks and citations omitted). The fact that the Act, which properly implements a valid treaty, reaches non-terrorism uses of chemical weapons leaves us powerless to excise such an individual instance. True, *Raich* involved Congress's Commerce Clause Power. But the Majority is correct to apply its principle to this case, particularly in light of the Supreme Court's rejection, in *Holland*, of federalism as a basis to challenge a statute implementing an otherwise valid treaty. See Maj. Op. at 166 n. 21; *Holland*, 252 U.S. at 432, 40 S.Ct. 382.

Ms. Bond continues to urge otherwise, asking us to consider the "world where the Supreme Court recognizes that the Tenth Amendment is primarily about protecting individual liberty," (3d Cir. Argument at 74), and to find controlling here cases like *New York v. United States*, 505 U.S. 144, 112 S.Ct. 2408, 120 L.Ed.2d 120 (1992), and *Printz v. United States*, 521 U.S. 898, 117 S.Ct. 2365, 138 L.Ed.2d 914 (1997), in which the Supreme Court recognized that some acts of Congress, even if they are otherwise valid under an enumerated power, can run afoul of the Tenth Amendment. But this case is not like *New York* or *Printz*, in which Congress wrongfully commandeered states' legislative processes and public officials. Nothing in those cases suggests a principle of federalism that would apply to this case.

Moreover, it is not enough to urge, as Ms. Bond does, that Pennsylvania law and authorities are equally able to handle, and punish, this conduct so that, from a federalism standpoint, we should leave the matter to Pennsylvania. That view simply misstates the law. We have a system of dual sovereignty. Instances of overlapping federal and state criminalization of similar conduct abound. But Ms. Bond argues that here, unlike the case with other federal crimes, no federal interest is being served by prosecuting every malicious use of a chemical. That argument fails for two reasons. First, there exists nowhere in the law a rule requiring that a statute implementing a treaty contain an element explicitly tying the statute to a federal interest so as to ensure that a particular application of the statute is constitutional. Cf. *United States v. Wilson*, 73 F.3d 675, 685 (7th Cir.1995) (reasoning that a jurisdictional element is not constitutionally required in a federal criminal statute enacted pursuant to Congress's Commerce Clause authority). Second, even if we were to require that there be a clear federal interest, Ms. Bond incorrectly characterizes the federal interest that is represented by her prosecution as one in prosecuting every malicious use of a chemical. Rather, the federal interest served is twofold: combating the use and proliferation of chemical weapons, and complying with the United States' obligations under a valid treaty. See Chemical Weapons Convention, art. VII.1, 32 I.L.M. 800, 810 (1993) (requiring each signatory nation to,

2. I agree with Ms. Bond that states sometimes also bear some responsibility for ensuring compliance with our treaty obligations. See *Medellin v. Texas*, 552 U.S. 491, 128 S.Ct. 1346, 170 L.Ed.2d 190 (2008). But that fact does not nullify Congress's authority to pass treaty-implementing legislation so as to ensure uniform, nationwide compliance with our international obligations, nor does it suggest that Congress lacks the power to do so.
“in accordance with its constitutional processes, adopt the necessary measures to implement its obligations under this Convention”). Additionally, whether there is a distinction, and where that distinction lies, between combating the use and proliferation of chemical weapons and prosecuting the malicious use of a chemical, is exceedingly difficult to discern.

In sum, Congress passed the Act, which is constitutionally sound legislation, to implement the Convention, a constitutionally sound treaty. Ms. Bond’s appeal generally to federalism, rather than to a workable principle that would limit the federal government’s authority to apply the Act to her, is to no avail.

The real culprits here are three. First, the fact pattern. No one would question a prosecution under the Act if the defendant were a deranged person who scattered potassium dichromate and 10–choloro–10H–phenoxarsine, the chemicals which Ms. Bond used, on the seats of the New York subway cars. While that defendant could be punished under state law, applying the Act there would not offend our sensibilities. The application, however, to this “domestic dispute,” somehow does.

Second, the “use” of chemical weapons as prescribed in the Act has an admittedly broad sweep. See Maj. Op. at 154 n. 7; Chemical Weapons Convention, art. VII.1(a), 32 I.L.M. at 810 (requiring each signatory nation to “[p]rohibit natural and legal persons anywhere on its territory . . . from undertaking any activity prohibited . . . under this Convention, including enacting penal legislation with respect to such activity”). Because the Act tracks the Convention, however, Congress had the power to criminalize all such uses. Perhaps, in carrying out the United States’ treaty obligations, Congress could have created a more expansive exception for “peaceful purposes,” but it did not.

Lastly, the decision to prosecute is troubling. The judgment call to prosecute Ms. Bond under a chemical weapons statute rather than allowing state authorities to process the case is one that we question. But we see that every day in drug cases. Perhaps lured by the perception of easier convictions and tougher sentences, prosecutors opt to proceed federally. See Steven D. Clymer, Unequal Justice: The Federalization of Criminal Law, 70 S. Cal. L.Rev. 643, 688–75 (1997). There is no law against this, or principle that we can call upon, to limit or regulate it.

While the Majority opinion explores arguments regarding the limits of the Treaty Power. I find Ms. Bond’s argument to be much more limited in scope, although equally unsupportable. I agree that we should affirm the judgment of the District Court.

AMBRO, Circuit Judge, concurring.

I concur in the result reached by Judge Jordan’s thoughtful opinion. I write separately to urge the Supreme Court to provide a clarifying explanation of its statement in Missouri v. Holland that “[i]f [a] treaty is valid there can be no dispute about the validity of the statute [implementing that treaty] under Article 1, Section 8, as a necessary and proper means to execute the powers of the Government.” 252 U.S. 416, 432, 40 S.Ct. 382, 64 L.Ed. 641 (1920).1

1. As I noted in our Court’s previous opinion in this case, see United States v. Bond, 581 F.3d 128, 135 (3d Cir.2009), rev’d in part by, Bond v. United States. — U.S. —, 131 S.Ct. 2355, 180 L.Ed.2d 269 (2011), the scope and persuasiveness of Holland has generated much academic debate. See, e.g., Nicholas Quinn Rosenkranz, Executing The Treaty Power, 118 Harv. L.Rev. 1867 (2005); Edward T. Swaine, Does Federalism Constrain the Treaty
Absent that undertaking, a blank check exists for the Federal Government to enact any laws that are rationally related to a valid treaty and that do not transgress affirmative constitutional restrictions, like the First Amendment. This acquirable police power, however, can run counter to the fundamental principle that the Constitution delegates powers to the Federal Government that are “few and defined” while the States retain powers that are “numerous and indefinite.” The Federalist No. 45 (James Madison).

Since Holland, Congress has largely resisted testing the outer bounds of its treaty-implementing authority. See Peter J. Spiro, Ressurrecting Missouri v. Holland, 73 Mo. L.Rev. 1029 (2008). But if ever there were a statute that did test those limits, it would be Section 229. With its shockingly broad definitions, Section 229 federalizes purely local, run-of-the-mill criminal conduct. The statute is a troublesome example of the Federal Government’s appetite for criminal lawmaking.2 Sweeping statutes like Section 229 are in deep tension with an important structural feature of our Government: “The States possess primary authority for defining and enforcing the criminal law.” Brecht v. Abrahamson, 507 U.S. 619, 635, 113 S.Ct. 1710, 123 L.Ed.2d 353 (1993) (quoting Engle v. Isaac, 456 U.S. 107, 128, 102 S.Ct. 1558, 71 L.Ed.2d 785 (1982)); see also Patterson v. New York, 432 U.S. 197, 201, 97 S.Ct. 2319, 53 L.Ed.2d 281 (1977) (“It goes without saying that preventing and dealing with crime is much more the business of the States than it is of the Federal Government. . . .”).

I hope that the Supreme Court will soon flesh out “[t]he most important sentence in the most important case about the constitutional law of foreign affairs,” Nicholas Quinn Rosenkranz, Executing The Treaty Power, 118 Harv. L.Rev. 1867, 1868 (2005), and, doing so, clarify (indeed curtail) the contours of federal power to enact laws that intrude on matters so local that no drafter of the Convention contemplated their inclusion in it.

John M. DEWEY; Patrick DeMartino; Patricia Romeo; Lynda Gallo; Ronald B. Marrans; Edward O. Griffin, on behalf of themselves and all others similarly situated

v.

VOLKSWAGEN AKTIENGESELLSCHAFT; Volkswagen Beteiligungs Gesellschaft M.B.H.; Volkswagen Group of America, Inc. (formerly known as Volkswagen of America, Inc.); Audi AG; Volkswagen Group of

2. “[T]he federal criminal code now includes at least 4,450 crimes. Congress added an average of 56.5 crimes per year to the federal code between 2000 and 2007 and has raised the total number of federal crimes by 40 percent since 1970. Moreover, the federal criminal code has grown not just in size but in complexity, making it difficult to both (1) determine what statutes constitute crimes and (2) differentiate whether a single statute with different acts listed within a section or subsection includes more than a single crime and, if so, how many.” John C. Eastman, The Outer Bounds of Criminal Law: Will Mrs. Bond Topple Missouri v. Holland?, 2011 Cato. Sup.Ct. Rev. 185, 193 (2011) (internal footnotes, quotation marks, and alterations omitted).
UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

NASSER AL-AULAQI,
as personal representative of the estates of
ANWAR AL-AULAQI and
ABDULRAHMAN AL-AULAQI
c/o American Civil Liberties Union
of the Nation’s Capital
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008,

SARAH KHAN,
as personal representative of the estate of
SAMIR KHAN
c/o American Civil Liberties Union
of the Nation’s Capital
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008,

Plaintiffs,

v.

LEON C. PANETTA,
Secretary of Defense
1000 Defense Pentagon
Washington, D.C. 20301-1000,

WILLIAM H. MCRAVEN,
Commander, Special Operations Command
7701 Tampa Point Boulevard
MacDill Air Force Base, FL 33621-5323,

JOSEPH VOTEL,
Commander, Joint Special Operations Command
P.O. Box 70239
Fort Bragg, N.C. 28307,

DAVID H. PETRAEUS,
Director, Central Intelligence Agency
Central Intelligence Agency
Washington, D.C. 20505,

All in their individual capacities,

Defendants.
COMPLAINT
(Violation of Fourth and Fifth Amendments and Bill of Attainder Clause – targeted killing)

INTRODUCTION

1. Since 2001, and routinely since 2009, the United States has carried out deliberate and premeditated killings of suspected terrorists overseas. The U.S. practice of “targeted killing” has resulted in the deaths of thousands of people, including many hundreds of civilian bystanders. While some targeted killings have been carried out in the context of the wars in Afghanistan and Iraq, many have taken place outside the context of armed conflict, in countries including Yemen, Somalia, Pakistan, Sudan, and the Philippines. These killings rely on vague legal standards, a closed executive process, and evidence never presented to the courts. This case concerns the role of Defendants Leon C. Panetta, William H. McRaven, Joseph Votel, and David H. Petraeus (collectively, “Defendants”) in authorizing and directing the killing of three American citizens in Yemen last year. The killings violated fundamental rights afforded to all U.S. citizens, including the right not to be deprived of life without due process of law.

2. In late 2009 or early 2010, Anwar Al-Aulaqi, an American citizen, was added to “kill lists” maintained by the Central Intelligence Agency (“CIA”) and the Joint Special Operations Command (“JSOC”), a component of the Department of Defense (“DOD”). On September 30, 2011, unmanned CIA and JSOC drones fired missiles at Anwar Al-Aulaqi and his vehicle, killing him and at least three other people, including Samir Khan, another American citizen. Defendants authorized and directed their subordinates to carry out the strike.
3. On October 14, 2011, Defendants authorized and directed another drone strike in Yemen, this one approximately 200 miles away from the strike that had killed Anwar Al-Aulaqi and Samir Khan two weeks earlier. The October 14 strike killed at least seven people at an open-air restaurant, including two children. One of the children was 16-year-old Abdulrahman Al-Aulaqi, who was Anwar Al-Aulaqi’s son and also an American citizen.

4. Defendants’ killing of Anwar Al-Aulaqi was unlawful. At the time of the killing, the United States was not engaged in an armed conflict with or within Yemen. Outside the context of armed conflict, both the United States Constitution and international human rights law prohibit the use of lethal force unless, at the time it is applied, lethal force is a last resort to protect against a concrete, specific, and imminent threat of death or serious physical injury. Upon information and belief, Anwar Al-Aulaqi was not engaged in activities that presented such a threat, and the use of lethal force against him was not a last resort. Even in the context of an armed conflict, the law of war cabins the government’s authority to use lethal force and prohibits killing civilians who are not directly participating in hostilities. The concept of “direct participation” requires both a causal and temporal nexus to hostilities. Upon information and belief, Defendants directed and authorized the killing of Anwar Al-Aulaqi even though he was not then directly participating in hostilities within the meaning of the law of war.

5. Defendants’ killing of Samir Khan and Abdulrahman Al-Aulaqi was also unlawful. Upon information and belief, neither Samir Khan nor Abdulrahman Al-Aulaqi was engaged in any activity that presented a concrete, specific, and imminent threat to life; nor was either of them directly participating in hostilities. The news media have
reported, based on statements attributed to anonymous U.S. government officials, that
Samir Khan was not the target of the September 30 strike and that Abdulrahman Al-
Aulaqi was not the target of the October 14 strike. If the Defendants were targeting
others, they had an obligation under the Constitution and international human rights law
to take measures to prevent harm to Samir Khan, Abdulrahman Al-Aulaqi, and other
bystanders. Even in the context of an armed conflict, government officials must comply
with the requirements of distinction and proportionality and take all feasible measures to
protect bystanders. Upon information and belief, Samir Khan and Abdulrahman Al-
Aulaqi were killed because Defendants failed to take such measures.

6. Plaintiffs are the personal representatives of the estates of Anwar Al-Aulaqi,
Samir Khan, and Abdulrahman Al-Aulaqi. They seek damages from Defendants for their
role in authorizing and directing the killings of Plaintiffs’ sons and grandson in violation
of the Fourth and Fifth Amendments and the Bill of Attainder Clause.

JURISDICTION AND VENUE

7. This complaint is for compensatory damages resulting from the conduct of
Defendants, all of them U.S. government officials, in violation of the Fourth and Fifth
Amendments and the Bill of Attainder Clause.

8. This Court has jurisdiction over this case pursuant to 28 U.S.C. § 1331
(federal question) and the U.S. Constitution.


PARTIES

10. Plaintiff Nasser Al-Aulaqi is the father of Anwar Al-Aulaqi and the
grandfather of Abdulrahman Al-Aulaqi. He is a citizen and resident of Yemen. He
brings this suit as the personal representative of the estates of his son and grandson, American citizens who were killed by missile strikes authorized and directed by Defendants.

11. Plaintiff Sarah Khan, an American citizen, is the mother of Samir Khan. She brings this suit as the personal representative of the estate of her son, an American citizen who was killed by missile strikes authorized and directed by Defendants.

12. Defendant Leon C. Panetta is the Secretary of Defense, a post he has held since July 2011. As Defense Secretary, he has ultimate authority over U.S. armed forces worldwide, including over JSOC. He authorized Anwar Al-Aulaqi’s continued placement on JSOC’s kill list after July 2011 and authorized and directed the missile strikes that killed Anwar Al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi. Between February 2009 and June 2011, Defendant Panetta was the Director of the CIA. As CIA Director, he authorized the addition of Anwar Al-Aulaqi to the CIA’s kill list. He is sued in his individual capacity.

13. Defendant William H. McRaven is Commander of the U.S. Special Operations Command (“USSOCOM”), a post he has held since August 2011. As Commander of USSOCOM, Defendant McRaven has authority over JSOC, a subordinate unified command within USSOCOM. He authorized and directed the missile strikes that killed Anwar Al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi. Between June 2008 and June 2011, he was the Commander of JSOC. In that capacity, he authorized the addition of Anwar Al-Aulaqi to JSOC’s kill list. He is sued in his individual capacity.

14. Defendant Joseph Votel is the Commander of JSOC, a post he has held since June 2011. As Commander of JSOC, he has authority over JSOC operations. He
authorized and directed the missile strikes that killed Anwar Al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi. He is sued in his individual capacity.

15. Defendant David H. Petraeus is the Director of the CIA, a post he has held since September 2011. As CIA Director, he has ultimate authority over the CIA’s operations worldwide. He authorized and directed the missile strikes that killed Anwar Al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi. He is sued in his individual capacity.

FACTUAL ALLEGATIONS

“Targeted Killings” by the United States

16. The first reported post-2001 targeted killing by the U.S. government outside Afghanistan occurred in Yemen in November 2002, when a CIA-operated Predator drone fired a missile at a terrorism suspect traveling in a car with other passengers. The strike killed all passengers in the vehicle, including an American citizen. The United Nations Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions later stated that the strike constituted “a clear case of extrajudicial killing” and set an “alarming precedent.”

17. Since 2002, the United States has continued to carry out targeted killings outside the context of armed conflict. The pace of these killings has increased dramatically since 2009. In the course of carrying out these killings, the government has killed many hundreds of civilian bystanders. In December 2009, a U.S. missile strike in the village of al-Majalah, Yemen, killed 41 people, including 21 children.

18. In April 2012, Deputy National Security Advisor John Brennan acknowledged publicly that the United States carries out targeted killings of suspected terrorists “beyond
hot battlefields like Afghanistan,” often using “remotely piloted aircraft” known as
“drones.” Both the CIA and JSOC are involved in authorizing, planning, and carrying
out these killings; both the CIA and JSOC have carried out such killings in Yemen; and,
according to a December 2011 report in the Washington Post and other news sources, the
CIA and JSOC “share intelligence and coordinate attacks.” Greg Miller, Under Obama,

19. Both the CIA and JSOC maintain “kill lists” setting out the names of the
individuals they intend to kill. See Jo Becker & Scott Shane, Secret ‘Kill List’ Proves a
Test of Obama’s Principles and Will, N.Y. Times, May 29, 2012. Upon information and
belief, the inclusion of an individual on one or both of the lists represents a standing order
authorizing and directing certain government personnel to kill that individual. In a
February 2011 interview with Newsweek, the CIA’s former acting general counsel John
Rizzo described the CIA’s list as “basically a hit list.” He stated that there are
approximately 30 individuals on the list “at any given time,” and that “[t]he Predator
(drone] is the weapon of choice, but it could also be someone putting a bullet in your

20. Senior government officials, including then-Director of National Intelligence
Dennis Blair and Deputy National Security Advisor John Brennan, have made clear that
the government’s claimed authority to carry out the targeted killing of suspected
terrorists, including killings executed outside the context of armed conflict, extends to
American citizens. However, government officials have offered incomplete and
inconsistent explanations of the legal standards that govern the placement of U.S. citizens
on the kill lists. Some officials have suggested that the U.S. government targets its
citizens only if they present “imminent” threats, but they have defined the term “imminent” so broadly as to negate its meaning.

**Defendants’ Decision to Authorize the Killing of Anwar Al-Aulaqi**

21. Plaintiff Nasser Al-Aulaqi is a Yemeni citizen who moved to the United States in 1966 to study as a Fulbright scholar at New Mexico State University. He and his wife lived in the United States until 1978, when they moved back to Yemen. In Yemen, he served as Minister of Agriculture and Fisheries and president of Sana’a University, and founded and served as president of Ibb University. He currently resides in Yemen with his wife, who is an American citizen, and their family.

22. Plaintiff Nasser Al-Aulaqi’s son, Anwar, was born in 1971 in New Mexico. He moved to Yemen with his parents in 1978. In 1991, he returned to the United States to attend college at Colorado State University. He obtained his master’s degree from San Diego State University and then enrolled in a Ph.D. program at George Washington University, which he attended through December 2001. While living in the United States, he married and had children, including Abdulrahman. He left the United States in 2003, first for the United Kingdom and then for Yemen.

23. In January 2010, the *Washington Post* reported that JSOC had added Anwar Al-Aulaqi to its kill list and had tried unsuccessfully to kill him in December 2009. Dana Priest, *U.S. Military Teams, Intelligence Deeply Involved in Aiding Yemen on Strikes*, Wash. Post, Jan. 27, 2010. Other media organizations reported the same information. In March 2010, the *Wall Street Journal* reported that then-CIA Director Defendant Panetta stated that Anwar Al-Aulaqi was “someone that we’re looking for” and that “there isn’t any question that he’s one of the individuals that we’re focusing on.” Keith Johnson,

24. The decision to add Anwar Al-Aulaqi to government kill lists was made after a closed executive process. Defendant Panetta participated in this process, and upon information and belief Defendant McRaven participated in this process as well. Upon information and belief, Defendants authorized and directed Anwar Al-Aulaqi’s killing even though, at the time lethal force was used, Anwar Al-Aulaqi was not engaged in activities that presented a concrete, specific, and imminent threat to life, and even though there were means short of lethal force that could reasonably have been used to address any such threat. Upon information and belief, Defendants authorized and directed Anwar Al-Aulaqi’s killing even though he was not then directly participating in hostilities within the meaning of the law of war.

25. In or around June 2010, the Department of Justice’s Office of Legal Counsel completed a memorandum providing legal justifications for the killing of Anwar Al-Aulaqi. Substantial portions of the memorandum were summarized in October 2011 by the New York Times, which reported, based on conversations with individuals who had read the document, that the memorandum “provided the justification for acting [against Anwar Al-Aulaqi] despite an executive order banning assassinations, a federal law against murder, protections in the Bill of Rights and various strictures of the international laws of war.” Charlie Savage, Secret U.S. Memo Made Legal Case to Kill a Citizen, N.Y. Times, Oct. 8, 2011.
26. Between the time Anwar Al-Aulaqi was added to the JSOC and CIA kill lists and the time he was killed, government officials told reporters that Al-Aulaqi had “cast his lot” with terrorist groups and encouraged others to engage in terrorist activity. Later, they claimed he had played “a key role in setting the strategic direction” for “Al Qaeda in the Arabian Peninsula (AQAP).” The government never publicly indicted Anwar Al-Aulaqi for any crime.

Nasser Al-Aulaqi’s Lawsuit to Enjoin the Government from Killing His Son

27. On August 30, 2010, Nasser Al-Aulaqi filed suit in this Court as next friend of his son, Anwar, asking that the Court enter an injunction barring the President, the CIA, and DOD (including JSOC) from carrying out the targeted killing of his son unless the executive concluded that he presented a concrete, specific, and imminent threat to life, and that there were no reasonably available measures short of lethal force that could be expected to address that threat. After hearing argument on November 8, 2010, the Court dismissed the Complaint on December 7, 2010, holding that Nasser Al-Aulaqi lacked standing to assert his son’s constitutional rights and that at least some of the issues raised by the Complaint were non-justiciable political questions. No appeal was taken.

Samir Khan


29. Samir Khan attended elementary school in Queens, New York, and high school on Long Island, New York. After graduating from high school in 2003, he moved
to North Carolina, where he attended a community college and worked part-time. He left for Yemen in October 2009.

30. Anonymous government officials have told reporters that Samir Khan was a “propagandist” for AQAP. The government never publicly indicted him for any crime.

The September 30, 2011 Killing of Anwar Al-Aulaqi and Samir Khan

31. On the morning of September 30, 2011, Anwar Al-Aulaqi and Samir Khan were in the Yemeni province of al-Jawf, some 90 miles northeast of Sana’a. Upon information and belief, Defendants Panetta, McRaven, Votel, and Petraeus authorized and directed personnel under their command to fire missiles at Anwar Al-Aulaqi and his vehicle from unmanned U.S. drones. The missiles destroyed the vehicle and killed Anwar Al-Aulaqi, Samir Khan, and at least two others. Witnesses reported that the missile strike left the vehicle a “charred husk” and “tore the [victims’] bodies to pieces.” Dominic Rushe, et al., Anwar al-Awlaki Death: US Keeps Role Under Wraps to Manage Yemen Fallout, Guardian, Sept. 30, 2011; Sudarsan Raghavan, Awlaki Hit Misses al-Qaeda Bombmaker, Yemen Says, Wash. Post, Sept 30, 2011. According to a September 30, 2011 article in the Washington Post and a June 2012 book by journalist Daniel Klaidman, personnel under Defendants’ command had been surveilling Anwar Al-Aulaqi for a period as long as three weeks leading up to the strike. Greg Miller, Strike on Aulaqi Demonstrates Collaboration Between CIA and Military, Wash. Post, Sept. 30, 2011; Daniel Klaidman, Kill or Capture (2012). Defendants’ lengthy surveillance suggests that the use of lethal force was not a last resort and that additional measures could have been taken to protect bystanders from harm.
32. The surveillance and the strike were carried out by the CIA and JSOC. Upon information and belief, Defendant Petraeus was personally responsible for authorizing and directing the CIA’s involvement in the September 30 strike, and Defendants Panetta, McRaven, and Votel were personally responsible for authorizing and directing JSOC’s involvement in it. Defendants coordinated with each other in planning the attack and carrying it out.

33. Senior government officials, including Defendant Panetta and President Barack Obama, have acknowledged the responsibility of the United States for killing Anwar Al-Aulaqi. On the same day the strike was carried out, DOD published a news article stating that “[a] U.S. airstrike . . . killed . . . Anwar [Al-Aulaqi] early this morning” and that he had been “high on the military-intelligence list of terrorist targets.” Lisa Daniel, Panetta: Awlaki Airstrike Shows U.S.-Yemen Cooperation, Am. Forces Press Service, Sept. 30, 2011. The following day, Defendant Panetta stated in a public speech that “it is because of th[e] teamwork between our intelligence and our military communities that we were successful in . . . taking down al-Awlaki.” Three weeks later, President Obama stated on national television that “working with the Yemenis, we were able to remove [Anwar Al-Aulaqi] from the field.” Tonight Show with Jay Leno (NBC television broadcast Oct. 25, 2011).

34. Defendants’ killing of Anwar Al-Aulaqi was unlawful. Upon information and belief, Defendants authorized and directed the strike even though, at the time the strike was carried out, Anwar Al-Aulaqi was not engaged in activities that presented a concrete, specific, and imminent threat of death or serious physical injury. Upon information and belief, Defendants authorized and directed the strike even though there were means short
of lethal force that could reasonably have been used to neutralize any threat that Anwar Al-Aulaqi’s activities may have presented. The killing of Anwar Al-Aulaqi was unlawful even if analyzed under the law of war because, upon information and belief, Defendants authorized and directed the strike even though Anwar Al-Aulaqi was not then directly participating in hostilities within the meaning of the law of war.

35. Defendants’ killing of Samir Khan was also unlawful. Samir Khan was not engaged in any activity that presented a concrete, specific, and imminent threat of death or serious physical injury; nor was he directly participating in hostilities. If he was killed because of the government’s targeting of Anwar al-Aulaqi, his killing was unlawful because Al-Aulaqi’s killing was unlawful and because, upon information and belief, Defendants authorized and directed the strike without taking legally required measures to avoid harm to bystanders. Even in the context of an armed conflict, government officials must comply with the requirements of distinction and proportionality and take all feasible measures to protect bystanders. Upon information and belief, Samir Khan was killed because Defendants failed to take such measures.

The October 14, 2011 Killing of Abdulrahman Al-Aulaqi

36. Plaintiff Nasser Al-Aulaqi’s grandson, Abdulrahman Al-Aulaqi, was born in Denver, Colorado, on August 26, 1995. He was raised in the United States until 2002, when he moved with his family to Yemen. At the time of his death, he was a student in his first year of high school and resided in Sana’a, Yemen, with his mother, siblings, grandmother, and grandfather.

37. On October 14, 2011, Abdulrahman was at an open-air restaurant near the town of Azzan, in the southern Yemeni province of Shabwa. Upon information and
belief, Defendants Panetta, McRaven, Votel, and Petraeus authorized and directed personnel under their command to fire missiles from unmanned U.S. drones at a person at or near the restaurant. According to media sources, the intended target was Ibrahim Al-Banna, an Egyptian national, but it was later reported that he was not among those killed by the strike. See Gregory Johnsen, *Signature Strikes in Yemen*, Waq al-Waq, Apr. 19, 2012. The strike killed at least seven people, including Abdulrahman and one of his cousins, another minor. Abdulrahman himself was 16 years old.

38. After the strike, a senior Obama administration official described Abdulrahman to the *Los Angeles Times* as a “military-aged male.” Ken Dilanian, *Grieving Awlaki Family Protests Yemen Drone Strikes*, L.A. Times, Oct. 19, 2011. Other news sources described Abdulrahman as a militant in his twenties. To correct these erroneous descriptions, Abdulrahman’s family provided his birth certificate to the *Washington Post*. After the *Washington Post* published the birth certificate, U.S. officials acknowledged in anonymous statements to the press that Abdulrahman had been a minor.

39. Upon information and belief, Defendant Panetta was personally responsible for authorizing and directing the CIA’s involvement in the October 14 strike, and Defendants Petraeus, McRaven, and Votel were personally responsible for authorizing and directing JSOC’s involvement in the October 14 strike. Defendants coordinated with each other in planning the attack and carrying it out.

40. The killing of Abdulrahman Al-Aulaqi was unlawful. Abdulrahman was not engaged in any activity that presented a concrete, specific, and imminent threat of death or serious physical injury; nor was he directly participating in hostilities. If he was killed because the government was targeting another individual, his killing was unlawful.
because, upon information and belief, Defendants authorized and directed the strike without taking legally required measures to avoid harm to him. Even in the context of an armed conflict, the government must comply with the requirements of distinction and proportionality and take all feasible measures to protect bystanders. Upon information and belief, Abdulrahman Al-Aulaqi was killed because Defendants failed to take such measures.

CAUSES OF ACTION

First Claim for Relief
Fifth Amendment: Due Process

41. Defendants’ actions described herein violated the substantive and procedural due process rights of Anwar Al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi under the Fifth Amendment to the Constitution. Defendants Panetta, McRaven, Votel, and Petraeus violated the Fifth Amendment due process rights of Anwar al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi by authorizing and directing their subordinates to use lethal force against them in the circumstances described above. The deaths of Anwar Al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi were a foreseeable result of Defendants’ actions and omissions.

Second Claim for Relief
Fourth Amendment: Unreasonable Seizure

42. Defendants’ actions described herein violated the rights of Anwar Al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi to be free from unreasonable seizures under the Fourth Amendment to the Constitution. Defendants Panetta, McRaven, Votel, and Petraeus violated the Fourth Amendment rights of Anwar al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi by authorizing and directing their subordinates to use lethal
force against them in the circumstances described above. The deaths of Anwar al-Aulaqi, Samir Khan, and Abdulrahman Al-Aulaqi were a foreseeable result of Defendants’ actions and omissions.

Third Claim for Relief
Bill of Attainder

43. Defendants’ actions described herein with respect to Anwar Al-Aulaqi violated the Constitution’s Bill of Attainder Clause. Defendants’ actions constituted an unconstitutional act of attainder because Defendants designated Anwar Al-Aulaqi for death without the protections of a judicial trial in the circumstances described above. The death of Anwar al-Aulaqi was a foreseeable result of Defendants’ actions and omissions.

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully request that this Court enter judgment awarding them:

A. Damages in an amount to be determined at trial; and

B. Such other relief as the Court deems just and proper.

Respectfully submitted,

/s/ Arthur B. Spitzer

Arthur B. Spitzer (D.C. Bar No. 235960)
American Civil Liberties Union
of the Nation’s Capital
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008
Telephone: (202) 457-0800; Fax: (202) 452-1868
art@aclu-nca.org

Jameel Jaffer (to be admitted pro hac vice)
Hina Shamsi (to be admitted pro hac vice)
Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 519-7814
jjaffer@aclu.org
Pardiss Kebriaei (to be admitted pro hac vice)
Maria C. LaHood (to be admitted pro hac vice)
Baher Azmy
Center for Constitutional Rights
666 Broadway, 7th floor
New York, NY 10012
(212) 614-6452
pkebriaei@ccrjustice.org

July 18, 2012
UNITED STATES COURT OF MILITARY COMMISSION REVIEW

BEFORE THE COURT EN BANC
BRAND, PRICE, SIMS, GALLAGHER, PERLAK, ORR, Appellate Military Judges

UNITED STATES OF AMERICA

v.

ALI HAMZA AHMAD SULIMAN AL BAHLUL

CMCR 09-001

September 9, 2011

Colonel Peter E. Brownback, II, JA, U.S. Army was the military commission judge through arraignment, and Colonel Ronald A. Gregory, U.S. Air Force, was the military commission judge for trial.

Michel Paradis argued the cause for appellant. With him on briefs were Major Todd E. Pierce, JA, U.S. Army, and Captain Mary McCormick, JAGC, U.S. Navy.

Captain Edward S. White, JAGC, U.S. Navy argued the cause for appellee. With him on briefs were Captain John F. Murphy, JAGC, U.S. Navy and Francis A. Gilligan.


PUBLISHED OPINION OF THE COURT

Opinion for the Court filed by PRICE, J., in which BRAND, GALLAGHER, SIMS, PERLAK, and ORR, JJ., concur.

1 Acting Chief Judge O'TOOLE and Judges THOMPSON, CONN, and GREGORY recused themselves from participation in appellant’s case. Judges GALLAGHER, HOFFMAN, PERLAK, and SIMS joined the Court on November 30, 2010. Judges ORR and GREGORY joined the Court on March 17, 2011. Judge HOFFMAN retired on August 1, 2011.
Judge Sims, filed a separate opinion, concurring.

I. INTRODUCTION .................................................................................................................. 4
II. PROCEDURAL HISTORY .................................................................................................... 4
III. JURISDICTIONAL BASIS FOR REVIEW ......................................................................... 6
IV. ISSUES ON APPEAL ......................................................................................................... 7
   A. Result of Court’s Review ............................................................................................... 8
V. STATEMENT OF FACTS .................................................................................................... 8
   A. The Al-Qaeda Plan ......................................................................................................... 9
   B. Appellant’s Background, Conduct, and Trial ............................................................... 11
VI. STANDARD OF REVIEW .................................................................................................. 15
VII. MILITARY COMMISSION SUBJECT MATTER JURISDICTION ................................. 15
   A. Introduction .................................................................................................................. 15
   B. Issue Presented ............................................................................................................ 18
   C. The Law ......................................................................................................................... 18
      1. Military Commissions Act of 2006 ........................................................................... 20
      2. Congressional Authority to Define and Punish Offenses
         Against the Law of Nations ..................................................................................... 21
      3. The Law of Nations .................................................................................................. 25
      4. The Law of Armed Conflict .................................................................................... 27
         a. Combatants—Lawful and Unlawful ................................................................. 30
            (1) Alien Unlawful Enemy Combatant (AUEC) –
                Common Element 1 ......................................................................................... 37
                (a) AUEC and the Law of Armed Conflict ...................................................... 39
                (b) Irregular Warfare ......................................................................................... 39
                (c) U.S. Army 1914 and 1956 Manuals .......................................................... 42
                (d) Terrorists ........................................................................................................ 44
                (e) Conclusion ...................................................................................................... 45
            (2) Conduct in the Context of and Associated with an
                Armed Conflict – Common Element 2 ......................................................... 45
VIII. PROVIDING MATERIAL SUPPORT FOR TERRORISM, EX POST
      FACTO, AND INSTRUCTIONAL ERROR ..................................................................... 47
   A. Providing Material Support for Terrorism – an Offense Under
      the Law of Armed Conflict ....................................................................................... 48
      1. The Charge .............................................................................................................. 48
      2. The 2006 M.C.A. and 2007 M.M.C. ................................................................... 50
         a. Material Support or Resources ......................................................................... 50
         b. Terrorism defined ............................................................................................... 52
      3. Non-U.S. Domestic Providing Material Support for
         Terrorism-Type Laws ............................................................................................ 57
   B. Discussion .................................................................................................................... 61
      1. Criminal Organizations – International Military Tribunal
         at Nuremberg .......................................................................................................... 63
      2. Control Council 10 – Nuremberg Military Tribunals ............................................. 65
      3. Joint Criminal Enterprise ..................................................................................... 71
   C. Analysis ......................................................................................................................... 76
   D. Complicity ..................................................................................................................... 78
   E. Aiding the Enemy .......................................................................................................... 79
F. Ex Post Facto ................................................................. 81
G. Instructional Error.......................................................... 82

IX. CONSPIRACY TO VIOLATE THE LAW OF WAR AS AN OFFENSE
    TRIABLE BY MILITARY COMMISSION.................................. 84
A. Conspiracy - The Charge and Specification........................... 86
B. Conspiracy under the 2006 M.C.A. and 2007 M.M.C.................... 87
C. Analysis........................................................................ 88
   1. Non-U.S. Conspiracy-Type Laws......................................... 93
D. Conclusion................................................................... 97

X. SOLICITATION AS AN OFFENSE TRIABLE BY
    MILITARY COMMISSION.................................................. 97
A. Solicitation - The Charge and Specification............................ 97
B. Solicitation under the 2006 M.C.A. and 2007 M.M.C.................... 98
C. Analysis........................................................................ 99
   1. Solicitation-Type Laws...................................................... 103

XI. FIRST AMENDMENT ISSUES.................................................. 111
A. Discussion.................................................................. 112
B. The Military Commissions Act and the First Amendment............ 115
C. Potential Chilling Effect on U.S. Citizens.............................. 120
D. Military Commission Judge’s Instructions............................ 121
E. Conclusion.................................................................. 122

XII. 2006 M.C.A. AND BILL OF ATTAINDER................................. 122
A. Bills of Attainder and Legislative Analysis............................ 122
   1. Legislatively Determines Guilt........................................... 123
   2. Legislatively Inflicts Punishment....................................... 123
      a. Historical Test.......................................................... 124
      b. Functional Test....................................................... 126
      c. Motivational Test.................................................... 126
         (1) Specificity of Identification.................................... 126
         (2) Lack of Judicial Trial............................................ 127
B. Conclusion.................................................................. 128

XIII. EQUAL PROTECTION........................................................ 128

XIV. WAIVER OF ASSIGNMENTS OF ERROR I, III to V..................... 128
A. The Law.................................................................... 129
B. Analysis.................................................................... 130

XV. SENTENCE APPROPRIATENESS........................................... 131
A. Applicable Law............................................................ 132
B. Analysis.................................................................... 133
   1. The Offense and the Offender.......................................... 133
   2. Closely-Related Cases.................................................. 136

XVI. CONCLUSION........................................................................ 138

Judge Sims concurring........................................................ 138
PRICE, JUDGE:

I. INTRODUCTION


A military commission comprised of military members determined that appellant was an alien unlawful enemy combatant, see infra nn. 23, 24, 53, and contrary to his pleas convicted him of: (1) providing material support and resources, including himself to al Qaeda, an international terrorist organization then engaged in hostilities with the United States with exceptions; (2) conspiring with Usama bin Laden and other members and associates of al Qaeda to, inter alia, commit murder, attack civilians and civilian objects in violation of the law of war, commit terrorism, and provide material support for terrorism with exceptions; and (3) soliciting various persons to commit these same offenses in violation of 2006 M.C.A. §§ 950v(b)(25), 950v(b)(28), and 950u. The members sentenced appellant to confinement for life and the convening authority approved the sentence.

II. PROCEDURAL HISTORY

One week after the September 11, 2001, attacks on the United States, Congress passed the Authorization for Use of Military Force resolution (AUMF). Pub. L. No. 107-40, 115 Stat. 224 (2001). The AUMF authorized the President to “use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks.” Id. The President ordered the Armed Forces to Afghanistan “to subdue Al Qaeda and quell the Taliban regime that was known to support it.” Hamdi v. Rumsfeld, 542 U.S. 507, 510 (2004).

In 2001, appellant was captured in Pakistan and turned over to the U.S. military. In 2002, he was transported to a military detention facility in Guantanamo Bay, Cuba, where he remains confined.

---


3 “Al Qaeda” is spelled “al Qaida” in some quotations. Either spelling is correct.

4 The members excepted the words, “Armed himself with an explosive belt, rifle, and grenades to protect and prevent the capture of Usama bin Laden.” Charge Sheet, Tr. 916-17.
In July 2003, the President declared appellant eligible for trial by military commission on unspecified charges pursuant to his Military Order. On February 23, 2004, the Deputy Appointing Authority referred to trial by military commission one charge and an accompanying specification alleging al Bahlul conspired with Usama bin Laden and other “members and associates of the al Qaeda organization, known and unknown, to commit” the offenses of “attacking civilians; attacking civilian objects; murder by an unprivileged belligerent; destruction of property by an unprivileged belligerent; and terrorism.” 2004 Charge Sheet and Referral.

On November 8, 2004, a Federal District Court stayed a military commission trial until the Department of Defense complied with various requirements of the Court. *Hamdan v. Rumsfeld*, 344 F. Supp. 2d 152, 173-74 (D.D.C. 2004). The same issues were present in appellant’s case, and on December 10, 2004, the Appointing Authority directed that appellant’s case be “held in abeyance” pending the outcome of the appeal filed in *Hamdan*.

On June 29, 2006, the Supreme Court ruled in *Hamdan v. Rumsfeld*, 548 U.S. 557, 635 (2006), that the military commission scheme then in existence violated Article 36, Uniform Code of Military Justice (UCMJ) and did not satisfy the requirements of Common Article 3 of the Geneva Conventions. Following the Supreme Court’s decision in *Hamdan*, the military commission judge abated the proceedings in appellant’s case. Tr. 8.


---


On February 26, 2008, the convening authority referred appellant’s charges and specifications to trial by military commission. Trial began on May 7, 2008. Following trial on the merits, during which appellant mounted no substantive defense, the military commission returned findings of guilty on each charge and specification and on November 3, 2008, sentenced appellant to confinement for life. On June 3, 2009, the convening authority approved the findings and sentence and ordered the sentence executed.


We recently decided the first direct appeal of a conviction by military commission convened under the 2006 M.C.A. United States v. Hamdan, ___ F. Supp. 2d ___, 2011 WL 2923945 (USCMCR June 24, 2011). In Hamdan, we concluded that the charged conduct of providing military support for terrorism was punishable under the law of armed conflict from at least February 1996, when Hamdan joined al Qaeda, that a rational basis existed for disparate treatment of aliens in the 2006 and 2009 M.C.A., and that such disparate treatment did not violate the Equal Protection Clause of the Constitution. 7

III. JURISDICTIONAL BASIS FOR REVIEW

The Court of Military Commission Review was authorized by Congress in the 2006 M.C.A. and established by the Secretary of Defense. The 2006 M.C.A. provides for “automatic referral” for review by this Court8 “each case in which the final decision of a military commission (as approved by the Convening Authority) includes a finding of ‘guilty.’”9 The 2006 M.C.A. limited our jurisdiction to act “to matters of law” and “[a] finding or sentence of a military commission under this chapter may not be held incorrect on the ground of an

---

7 These three issues were substantially addressed in our Court’s decision in Hamdan, 2011 WL 2923945. For purposes of readability, portions of that decision are quoted in this decision without formatting as quotations and sometimes without citation to that decision. Nothing in this decision should be construed as inconsistent with or limiting the Court’s decision in Hamdan.

8 Except in a case in which the approved sentence extends to death, an accused may expressly waive appellate review. 2006 M.C.A. § 950c(b); 2009 M.C.A. § 950c(b).

error of law unless the error materially prejudices the substantial rights of the accused.” 2006 M.C.A. §§ 950f(d) and 950a(a).\textsuperscript{10}

In section 950f(a) of the 2009 M.C.A., Congress designated our Court as the United States Court of Military Commission Review, and significantly expanded the scope of our review authority in cases automatically referred for appellate review. In addition to the authority to act with respect to “matters of law,” the 2009 M.C.A. § 950f(d), requires us to review the record for factual sufficiency and sentence appropriateness:

The Court may affirm only such findings of guilty, and the sentence or such part or amount of the sentence, as the Court finds correct in law and fact and determines, on the basis of the entire record, should be approved. In considering the record, the Court may weigh the evidence, judge the credibility of witnesses, and determine controverted questions of fact, recognizing that the military commission saw and heard the witnesses.

This expanded authority mirrors that exercised by the military service Courts of Criminal Appeals in review of courts-martial in which the approved sentence includes death, a punitive discharge, or confinement for one year or more, an authority characterized as an “awesome, plenary, de novo power of review.” United States v. Cole, 31 M.J. 270, 272 (C.M.A. 1990) (citing 10 U.S.C. § 866). We apply the standards and scope of review in the 2009 M.C.A. §§ 950a(a) and 950f(d), as it is more favorable to appellant. See Hamdan, 2011 WL 2923945 at *9 n. 15 (citations omitted).

We have jurisdiction over this case because the final decision of the military commission, as approved by the convening authority, includes findings of “guilty.” See supra n. 9.

IV. ISSUES ON APPEAL

Appellant raises six assignments of error that merit discussion. First, that his convictions must be reversed as none of his charged offenses constitute war crimes triable by military commission. Second, that his conviction for providing material support for terrorism must be reversed as that charge violated the Ex

\textsuperscript{10} See also Article 59(a), Uniform Code of Military Justice (UCMJ) (“A finding or sentence of court-martial may not be held incorrect on the ground of an error of law unless the error materially prejudices the substantial rights of the accused.”); Fed. Rule Crim. Proc. 52 (stating, a “harmless error” is “[a]ny error, defect, irregularity, or variance that does not affect substantial rights.” Harmless errors “must be disregarded,” and “plain error” is an “error that affects substantial rights.” Plain error “may be considered even though it was not brought to the court’s attention.”); cf, 28 U.S.C. § 2106 (stating, “The Supreme Court or any other court of appellate jurisdiction may affirm, modify, vacate, set aside or reverse any judgment, decree, or order of a court lawfully brought before it for review, and may remand the cause and direct the entry of such appropriate judgment, decree, or order, or require such further proceedings to be had as may be just under the circumstances.”).
Post Facto Clause of the U.S. Constitution and the term “material support” was erroneously defined by the military commission judge. Third, that he was convicted on the basis of political speech in violation of the First Amendment of the U.S. Constitution. Fourth, that the 2006 M.C.A. is an unconstitutional Bill of Attainder. Fifth, that the 2006 M.C.A. violates the Constitution’s Equal Protection Clause by making aliens, but not citizens, subject to trial by military commission. Sixth, that a sentence of life imprisonment is inappropriately severe and disproportionate to the sentences of closely-related defendants. We specified two issues.\(^{11}\)

A. Result of Court’s Review

We have carefully considered the record, the various pleadings and oral arguments of the parties. We hold that the findings and sentence are correct in law and fact and that no error materially prejudicial to the substantial rights of appellant occurred. 2009 M.C.A. §§ 950a(a) and 950f(d).

V. STATEMENT OF FACTS

Appellant, a self-described “officer” in al Qaeda, joined that group with knowledge that al Qaeda engaged in terrorism and did so in complete agreement with Usama bin Laden’s declarations that all Americans and anyone in the United States were legitimate targets of armed attack. Following completion of al Qaeda’s military-like training, appellant met personally with bin Laden, discussed al Qaeda’s view of itself as a government in exile for the Muslim world engaged in jihad (or “holy war”) with the United States, and pledged his personal fealty, including his willingness to die for bin Laden and al Qaeda.

Bin Laden then assigned appellant to al Qaeda’s media office and later as his personal assistant/secretary for public relations. Appellant’s conduct in those positions and membership in al Qaeda provide the factual basis for his convictions of: (1) providing material support and resources to al Qaeda; (2)

\(^{11}\) The two specified issues are as follows:

I. Assuming that Charges I, II, and III allege underlying conduct (e.g., murder of protected persons) that violates the law of armed conflict and that “joint criminal enterprise” is a theory of individual criminal liability under the law of armed conflict, what, if any, impact does the “joint criminal enterprise” theory of individual criminal liability have on this Court’s determinations of whether Charges I through III constitute offenses triable by military commission and whether those charges violate the Ex Post Facto clause of the Constitution? See, e.g., Hamdan v. Rumsfeld, 548 U.S. 557, 611 n. 40 (2006).

II. In numerous Civil War and Philippine Insurrection cases, military commissions convicted persons of aiding or providing support to the enemy. Is the offense of aiding the enemy limited to those who have betrayed an allegiance or duty to a sovereign nation? See Hamdan v. Rumsfeld, 548 U.S. 557, 600-01, n. 32, 607, 693-97 (2006).
conspiring with bin Laden and others to, *inter alia*, commit murder, attack civilians and civilian objects, commit terrorism, and provide material support for terrorism; and (3) soliciting various persons to commit those same offenses.

A brief review of al Qaeda’s history, organization and goals is essential to put appellant’s conduct in context.

A. The Al-Qaeda Plan

In December 1979, the former Soviet Union invaded Afghanistan. The Soviets were soon opposed by the mujahideen (self-proclaimed Muslim “holy warriors”), including native Afghans and volunteers for the proclaimed jihad against the Soviet Union. By 1985 radical Palestinian cleric Dr. Abdullah Azzam emerged as leader of the Arab recruits. “Azzam and his supporters schemed to use the conflict in Afghanistan as a means to create a multi-national Muslim army to wipe out secular regimes across the Middle East, Asia and North Africa,” and to establish an Islamic Caliphate. “In April 1988, Azzam published [a] manifesto, titled ‘Al-Qaida’, meaning ‘The Base’ or ‘the Solid Foundation,’” in which he advocated armed struggle:

Azzam reasoned that every revolutionary ideology needs a rugged, elite cadre to protect it, inspire it, and lead it to ultimate victory . . . . Azzam issued what he referred to as “the final call”: “We shall continue the Jihad no matter how long the way is until the last breath and the last beating of the pulse or we see the Islamic state established.”

“[M]illionaire Saudi exile Usama Bin Laden . . . provided . . . financing and logistical support to Azzam’s organization and soon . . . became a dominant force among the Arabs fighting in Afghanistan. . . . On September 10, 1988, Azzam, bin Laden, and mujahideen convened the first meeting of al Qaeda.” The leaders of al Qaeda formed a Shura (Advisory Council) and divided operations “amongst various wings, including a military committee, a security committee, a financial committee, a religious legal committee, a political committee, and a media committee.”

Following withdrawal of Soviet troops from Afghanistan, the varying mujahideen factions turned on each other and Dr. Azzam died. In 1991, facing collapse of the armed struggle in Afghanistan, bin Laden moved to Sudan, set up business enterprises and sponsored overseas terrorist activities. Al Qaeda’s leaders were angered by American troop presence in Saudi Arabia following the 1991 Persian Gulf War and “believed that Islamic doctrine prohibits the

---

12 Unless otherwise stated, the facts and quotations in this section are from Prosecution Ex. 14A, which is the “Script: ‘The Al-Qaida Plan’” by Evan F. Kohlmann, or from Mr. Kohlmann’s testimony at trial. Tr. 750-815.
presence of infidels, or non-Muslims, in the 'Land of the Two Holy Places' . . . , the Arabian Peninsula, home to the sacred Muslim cities of Mecca and Medina."

In December 1991, following a "fatwa" (religious edict) issued on behalf of al Qaeda condemning the presence of U.S. military peacekeepers, militants attempted to attack U.S. soldiers in Yemen who were en route to Somalia peacekeeping duties. In 1993, bin Laden announced that "the American army now they came to the Horn of Africa, and we have to stop the head of the snake . . . the snake is America and we have to stop them. We have to cut the head and stop them." Later that year, Somali militiamen, some of whom were al Qaeda-trained, shot down two U.S. Blackhawk helicopters over Mogadishu, and 18 U.S. servicemen were killed in the ensuing battle.

In 1996, the Sudanese regime ordered bin Laden and his associates out of Sudan. They relocated to Afghanistan at the invitation of the Taliban. In August 1996, bin Laden published a "declaration of war" in which he wrote:

It is now clear that those who claim that the blood of the American soldiers (the enemy occupying the land of the Muslims) should be protected are merely repeating what is imposed on them by the regime; fearing the aggression and interested in saving themselves. It is a duty now on every tribe in the Arab Peninsula to fight, Jihad, in the cause of Allah and to cleanse the land from those occupiers. Allah knows that the[ir] blood is permitted (to be spilled) and their wealth is a booty to those who kill them. . . . Death is better than life in humiliation! . . . My Muslim Brothers of The World: Your brothers . . . are calling upon your help and asking you to take part in fighting against the enemy—your enemy and their enemy—the Americans and the Israelis. They are asking you to do whatever you can . . . to expel the enemy, humiliated and defeated, out of the sanctities of Islam.

In February 1998, bin Laden and like-minded allies founded the World Islamic Front Against Jews and Crusaders and signed a joint fatwa requiring all able Muslims to kill Americans - whether civilian or military - anywhere they can be found and to "plunder their money." On May 29, 1998, bin Laden issued a second declaration entitled "The Nuclear Bomb of Islam," in which he stated that "it is the duty of the Muslims to prepare as much force as possible to terrorize the enemies of God."

On August 7, 1998, U.S. embassies in Kenya and Tanzania were suicide-bombed by al Qaeda operatives, resulting in 257 deaths including 12 Americans. On August 20, 1998, the U.S. responded by striking terrorist training camps and a suspected chemical weapons laboratory. In October 1999, the U.S. Government officially designated al Qaeda a foreign terrorist organization, making it unlawful for anyone in the United States to provide material support
to al Qaeda, and froze al Qaeda linked resources held by U.S. financial institutions.

In January 2000, al Qaeda attempted an attack on the USS THE SULLIVANS near Yemen; however, the attack boat was overloaded and sank. That boat was recovered and on October 12, 2000, disguised as a friendly civilian boat welcoming the USS COLE to port, suicide-detonated against the COLE, killing 17 American sailors, wounding 39 others, and extensively damaging the ship.

On September 11, 2001, 19 men recruited by al Qaeda hijacked four commercial airliners in the United States and intentionally crashed one airliner into the Pentagon in Washington, D.C. and two into the World Trade Center in New York. The fourth aircraft crashed in Pennsylvania after the passengers attempted to retake the plane from the hijackers. Thousands of Americans and others were killed as a result of the September 11, 2001 attacks.

B. Appellant’s Background, Conduct, and Trial

Born in Yemen on September 11, 1969, appellant is well-educated and speaks some English. In the early 1990s he was inspired by Azzam’s speeches and traveled to Afghanistan to fight the Soviet-supported regime. He then returned to Yemen.

In the late 1990s, appellant approached a known al Qaeda member in Yemen about returning to Afghanistan. He used money and a visa provided by al Qaeda operatives and traveled to Afghanistan. After completing military-like training, appellant talked to and pledged bayat to bin Laden and joined al Qaeda. Bin Laden then assigned him to al Qaeda’s media office.

Following the October 2000 attack on the USS COLE, bin Laden instructed appellant to prepare a video exploiting that attack for recruiting purposes. This full-length video, entitled “The Destruction of the American Destroyer Cole,” is comprised of extensive footage intended to inflame the viewers and incite them to migrate to Afghanistan to train for, and actively participate in, violent jihad against the United States. Appellant was proud of the video, claiming it was al Qaeda’s best propaganda video at that time, and that it “was influential” and produced “a good result” for al Qaeda. Tr. 534. Translated into multiple languages and widely distributed outside Afghanistan, the video demonstrated power to incite persons with no prior connection to al Qaeda to action. The video is organized into three parts: “The Problem,” “The Causes,” and “The Solution.”

“The Problem” is appellant’s portrayal of the Muslim nation or “Ummah” and includes emotive footage of purported Muslims, particularly women and children, being mistreated and killed. It also depicts the presence of U.S.
diplomats and troops in the Middle East as part of “The Problem.” The video identifies “The Causes” as diplomatic relationships between the United States and regional leaders and an alliance between the United States and Israel.

“The Solution” includes incensing images of violence against women and children, interspersed with images of world leaders including American Presidents laughing. The horrific and infuriating images are shown repeatedly with religious chanting and “a cappella” singing, known as “anasheeds,” audible in the background to increase the emotional impact of the video. The anasheed extol the virtues of martyrdom (suicide bombings), of sacrifice, and of combat, somberly chanting lyrics such as “revolt, revolt . . . with blood, with blood.” Tr. 809. The anasheed instructs the listener to trade blood for blood and destruction for destruction, while showing images of violence against women and children dying, then images of recruits training in al Qaeda camps and terrorist attacks on Americans, and finally joyful Muslims celebrating in the streets. After highly emotional scenes of Muslims suffering attributed to “Western infidels” and complicit Middle Eastern regimes, the video asserts violent jihad as the solution. It calls on viewers to come to Afghanistan to train for, and actively participate in, violent jihad against the United States.

During training camp scenes, bin Laden says, “the outcome of this training is jihad for the cause of God. . . . [T]hey are waiting for our youths to annihilate America and Israel.” Prosecution Ex. 31 at 15. He continues, “[t]he only way to eradicate the humiliation and disbelief that has overcome the Land of Islam is jihad, bullets, and martyrdom operations.” Id. at 16. Toward the end of the video, bin Laden declares, “[w]e are terrorists, and terror is an obligation in the Book of God. Let the West and East know that we are terrorists and we strike fear.” Id. at 18.

Appellant explained the importance he and bin Laden ascribed to appellant’s role as a “media man” in supporting al Qaeda’s objectives:

I was bored when I was in Afghanistan and working on computers and papers and cameras and TVs; and I asked bin Laden for a martyrdom operation, suicide operation; but he refused. The reason why he refused was that he--that there are many other people other than you or so--the recruiting people through media gets you more people than suicidal attacks.

Even in America, in every country in the world, media is the master ministry or department; and it has strategic goals, just like the United Nations and Internal Affairs and the Treasury Department; and God bless us, his speech was right.

Tr. 195.
After work on the video was completed, bin Laden appointed appellant as his personal assistant and secretary for public relations. Appellant assisted bin Laden in preparing public statements. He operated and maintained data processing equipment, arranged for Mohammad Atta and Ziad al Jarrah (two 9/11 hijackers/pilots) to pledge fealty to bin Laden, and prepared propaganda declarations styled as “martyr wills” to motivate those individuals to commit the 9/11 attacks and document al Qaeda’s role in those attacks.

Before the 9/11 attacks bin Laden ordered al Qaeda’s Kandahar site evacuated, and told appellant to ready the media van, which included computer, satellite, television, and radio communications equipment. Appellant evacuated Kandahar and traveled in a vehicle convoy, which included bin Laden and other al Qaeda leaders. On 9/11, appellant was unable to obtain a video signal, so bin Laden and other al Qaeda leaders first heard reports of the 9/11 attacks via a radio operated by appellant. At bin Laden’s request, appellant researched the economic impact of the 9/11 attacks and provided the results of his research to bin Laden.

Following his capture, appellant voluntarily spoke with multiple investigators regarding his background and role in al Qaeda, including his membership, status as an officer, role in production of the COLE video, and belief in bin Laden’s 1996 “declaration of war.” Appellant advised investigators that he was willing to discuss his own actions but unwilling to discuss those of others. Prosecution Ex. 13 at 4. He admitted committing each charged act. He also wrote several letters while detained at Guantanamo Bay to al Qaeda leaders renewing his pledge of bayat, restating his resolve to fight to the end, and reaffirming his belief that war is the only way to secure al Qaeda’s objectives. Prosecution Ex. 15-18. In Prosecution Ex. 18, he stated:

The days go on, the war will wage, the conflict will continue, the blood did not and will never dry, and the fate of their [American] utmost interests of their civilization is tied to and mortgaged by our Islamic region . . . They and their strategic allies have opened a big door that will not be closed until we regain our occupied holy places – the war is long and we are still at the beginning . . . democracy is on its death bed and it is about to succumb to its demise.

Appellant objected to the legitimacy of the military commission that tried him and indicated his intent to boycott the proceedings. He also objected to representation by counsel detailed by the Chief Defense Counsel of Military Commissions. He expressed a desire to proceed pro se and represent himself. Appellant also expressed his aspiration to absent himself from all sessions of the military commission, except he wanted to attend the final session to hear announcement of his sentence. The military commission judge advised appellant that his voluntary absence would constitute “waiver of the right to be present,” that his absence “could negatively impact the presentation of [his] case,” and
that his absence would be inconsistent with representing himself and would provide a basis to terminate his proceeding pro se. Appellant conveyed his understanding stating "[t]his is my final decision, and it's voluntary[]y and I've chosen that." Tr. 78.

Following this colloquy, appellant absented himself from the next session of court on August 15, 2008. The military commission judge then noted appellant's voluntary absence, particularly with respect to the pro se issue. Major Frakt, appellant's detailed defense counsel, represented to the military commission judge that he discussed his willingness to "defend [appellant] in the manner in which [appellant] desired to be defended." Tr. 80. Major Frakt also confirmed he had discussed the pro se representation issue with appellant, that appellant understood the impact of his voluntary absence from proceedings on his request to proceed pro se, and then Major Frakt related that appellant expressed "his very strong desire to return to the detention facility and to have no further communication with counsel of any kind." Tr. 80. In light of appellant's stated boycott and voluntary absence, the military commission judge ruled that detailed defense counsel, Major Frakt, would continue to represent appellant. Appellant's defense counsel then commented, "In accordance with Mr. Al Bahlul's wishes, defense demands, under Rule for Military Commission 707, a speedy trial. The defense waives all pretrial motions of any kind and is prepared to go to trial at the soonest possible date." Tr. 85.

Appellant's posturing, equivocation about his exercise of the right to counsel and proceeding pro se, and variable attendance have combined to create a significant ambiguity in the record. Detailed defense counsel, whose services were ostensibly rejected by appellant at the preceding session of court, appeared on August 15, 2008, without appellant present, putatively representing appellant's wishes. This ambiguity informs our treatment of the matters of waiver and forfeiture, discussed in Part XIV, infra at p. 128.

Appellant attended the next session of court on September 24, 2008, and expressed his preference to attend the trial if such attendance would not forfeit his boycott. The military commission judge informed appellant that his attendance would not forfeit his stated boycott, and appellant attended all subsequent proceedings. Appellant entered pleas of not guilty to all charges and specifications. With the exception of administrative matters and appellant's unsworn statement and related documents presented during the presentencing hearing, appellant presented no defense, made no closing argument, interposed no objection to prosecution evidence, conducted no cross-examination of prosecution witnesses, and presented no defense evidence.

In an unsworn statement to the members during the presentencing hearing, appellant acknowledged his membership in al Qaeda, asserting "we are the only ones on earth who will stand against you," the United States was responsible for the deaths of innocent civilians for 50 years and as such "we give you the same
cup you have given us[.]” Tr. 968-69. He declared that al Qaeda does not submit to any Arab government or to international law, only to God. He also commented that 9/11 was the consequence of U.S. Government policies, and he expressed his willingness to die in prison and belief that al Qaeda will prevail in its war against the United States. He then cited a poem penned by bin Laden named “The Storm of the Airplanes”:

Then the war is ongoing. It’s not going to be stopped and until you become fair and go back to your country and pull your ships from the peninsula ... As long as you occupy the Islam island in a direct way or an indirect way and you are around it from the sea and by land and by air, we will continue the war. ... [A]s a media man in al Qaeda, we actually take the words into action; and the members of 9/11, they were all media men before they became military men; and I was number 20, but bin Laden refused. My presence here today, I tell you: Sentence me the way you choose. It’s not going to stop us from saying the word of truth. Any power--we consider America as a tiger made out of paper. Yes, there is a weight for its force, but we are not scared of it. We are only scared of his almighty God. . . .

Tr. 978-79. The members sentenced appellant to confinement for life.

VI. STANDARD OF REVIEW

On appeal, appellant challenges the authority of Congress to legislate and the President, or his designee, to implement the 2006 M.C.A., on a number of constitutional grounds. He also alleges that the military commission judge misapplied the law and that the sentence awarded is inappropriately severe. Whether a military commission may exercise jurisdiction over the charged offenses is a question of law we review de novo. Defenders of Wildlife v. Gutiérrez, 532 F.3d 913, 919 (D.C. Cir. 2008); Hamdan, 2011 WL 2923945 at *9; United States v. Khadr, 717 F. Supp. 2d 1215, 1220 (USCMCISR 2007). Challenges to the constitutionality of the 2006 M.C.A. are reviewed de novo. Hamdan, 2011 WL 2923945 at *9 n. 14 (citations omitted). We also review sentence appropriateness and factual sufficiency de novo.13

VII. MILITARY COMMISSION SUBJECT MATTER JURISDICTION

A. Introduction

Appellant alleges that his convictions must be reversed because none of the charges constitute war crimes triable by military commission. Brief for

Appellant 21-28; Reply Brief for Appellant 11-13. Brief on Specified Issues for Appellant 6-39; Reply Brief on Specified Issues for Appellant 5-31. He argues that the military commission’s subject matter jurisdiction is limited to war crimes, that Congress’ authority to define and punish offenses triable by military commission is constrained to those offenses internationally recognized as violations of the law of war, and that none of the offenses of which he stands convicted are so recognized. *Id.* Appellant, in essence, asserts that Congress exceeded the scope of its constitutional authority in making the offenses of which he was charged and convicted punishable by military commission. *Id.*

Appellee replies that the military commission validly exercised jurisdiction over the charged offenses. Brief for Appellee 16-30; Brief on Specified Issues for Appellant 1-31. Specifically, that the constitutional authority to define and punish offenses against the law of nations is vested in Congress, that the authority to determine the jurisdiction of military commissions belongs to the political branches exercising their war powers, and that exercise of that authority is entitled to great deference. *Id.* In addition, appellee asserts that even if a military commission’s jurisdiction is limited to common law of war offenses, appellant stands convicted of conduct which violates the common law of war. *Id.* at 19-30.

Appellant’s challenge of Congress’ constitutional authority to “define” his conduct as an offense raises fundamental and significant questions as to the scope of legislative and executive authority in this area and as to what, if any, deference is due the exercise of that authority by reviewing courts. Our review is guided by two fundamental principles. First, the canon of “constitutional avoidance,” that being “when the constitutionality of a statute is assailed, if the statute be reasonably susceptible of two interpretations, by one of which it would be unconstitutional and by the other valid, it is our plain duty to adopt that construction which will save the statute from constitutional infirmity.” 14 Second, we are also guided by the long-standing principle that “an act of Congress ought never to be construed to violate the law of nations if any other possible construction remains . . . .” *Murray v. Schooner Charming Betsy*, 6 U.S. 64, 118 (1804).

The offenses of which appellant stands convicted were explicitly defined, as such, by Congress in coordination with the President following the Supreme Court’s decision in *Hamdan*, and explicitly intended to address punishment of those with whom the United States was and remains engaged in armed conflict. In the words of Justice Jackson, when national security relating to foreign

---

14 *Skilling v. United States*, 130 S. Ct. 2896, 2940, 177 L.Ed.2d 619, 659 (2010) (citing *United States ex rel. Attorney General v. Delaware & Hudson Co.*, 213 U.S. 366, 407 (1909)); see also id. 130 S. Ct. at 2930, 177 L.Ed.2d at 669 (citing *United States v. Harriss*, 347 U.S. 612, 618 (1954) (“[I]f the general class of offenses to which the statute is directed is plainly within its terms, the statute will not be struck down as vague . . . . And if this general class of offenses can be made constitutionally definite by a reasonable construction of the statute, this Court is under a duty to give the statute that construction.”)).
affairs is an issue, "[an action] executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it." Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring; citations omitted; quoted at infra n. 29). See also Hamdan, 2011 WL 2923945 at *12 and n. 27.

In the 2006 M.C.A., Congress endeavored “to enumerate or define by statute” the acts punishable by military commission in a conflict characterized by the Supreme Court as “not of an international character occurring in the territory of one of the High Contracting Parties.” See Hamdan, 548 U.S. at 629. This is an area of law where explicit international treaty law is generally characterized as “rudimentary” and customary international law is appropriately described as evolving.15 The parties’ acknowledgement that Congress, with the full support of the President, developed a comprehensive code to define and punish the conduct of widely disparate individuals in a global-battle space also informs our analysis.

Even cursory review of the 2006 M.C.A. reveals that Congress cast a wide net of potential individual criminal liability with respect to the offenses which may be subject of trial by military commission.16 Of course, we need not, and jurisprudentially speaking, indeed should not, attempt to define the outer edges or margins of this plainly broad net unless required to do so by a specific issue in controversy.17


17 United States v. Denedo, 556 U.S. ___, 129 S. Ct. 2213, 2221 (2009) (In discussing the scope of the All Writs Act, 28 U.S.C. § 1651(a), the Court stated, “a court’s power to issue any form of relief--extraordinary or otherwise--is contingent on that court’s subject-matter jurisdiction over the case or controversy. Assuming no constraints or limitations grounded in the Constitution are implicated, it is for Congress to determine the subject-matter jurisdiction of federal courts. Bowles v. Russell, 551 U.S. 205, 212, 127 S. Ct. 2360, 168 L. Ed. 2d 96 (2007) (“Within constitutional bounds, Congress decides what cases the federal courts have jurisdiction to consider”). This rule applies with added force to Article I tribunals, such as the NMCCA and CAAF, which owe their existence to Congress’ authority
In addition, the hybrid nature of international terrorism presents unique legal and policy challenges as the underlying conduct is often punishable under the law of nations, the domestic law of civilized nations, or both. Consideration of the aforementioned, particularly in this statutorily prescribed, yet nascent military commissions system “requires us to proceed with circumspection.”

B. Issue Presented

Accordingly, we see the jurisdictional issue presented as similar to that addressed in Ex parte Quirin, “[w]e are concerned only with the question whether it is within the constitutional power of the National Government to place [appellant] on trial before a military commission for the offenses charged.” Ex parte Quirin, 317 U.S. 1, 29 (1942). More specifically, we will focus on the charged conduct in each specification and “inquire whether any of the acts charged is an offense against the law of war cognizable before a military tribunal, and if so whether the Constitution prohibits the trial.” Id.; see also Ex Parte Milligan, 71 U.S. 2, 45 (1866). We will discuss the issues of law common to the offenses of which appellant stands convicted and address whether each individual offense describes conduct punishable by military commission.

C. The Law

“Congress and the President, like the courts, possess no power not derived from the Constitution.” Quirin, 317 U.S. at 25. The Constitution invests in Congress the authority to:

provide for the common Defence, Art. I, § 8, cl. 1, . . . To make Rules for the Government and Regulation of the land and naval Forces, Art. I, § 8, cl. 14, . . . To define and punish Piracies and Felonies committed on the high Seas, and Offenses against the Law of Nations, Art. I, § 8, cl. 10,

to enact legislation pursuant to Art. I, § 8 of the Constitution. [Clinton v.] Goldsmith, 526 U.S. [529], 533-534 [(1999)].”.

Hamdan, 2011 WL 2923945 at *12; See also United States v. Chisholm, 59 M.J. 151, 152 (C.A.A.F. 2003) (“Courts established under Article I of the Constitution, such as this Court, generally adhere to the prohibition on advisory opinions as a prudential matter.”)(citing United States v. Clay, 10 M.J. 269 (C.M.A. 1981); Munaf v. Geren, 553 U.S. 674, 689 (2008) (quoting Romero v. International Terminal Operating Co., 358 U.S. 354, 383 (1959))(The nature of the issues raised “requires us to proceed ‘with the circumspection appropriate when . . . adjudicating issues inevitably entangled in the conduct of our international relations.”).

Consistent with our statutory mandate to “affirm only such findings of guilty . . . as [we] find[] correct in law and fact and determine[], on the basis of the entire record, should be approved,” we will assess each charge and underlying specification. 2009 M.C.A. § 950f(d).
... [and] To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof. Art. I, § 8, cl. 18.

_Id_. at 26. In addition, the Constitution authorizes Congress "To constitute Tribunals inferior to the Supreme Court." U.S. Const., art. I, § 8, cl. 9.

"The Constitution confers on the President the 'executive Power,' Art. II, § 1, cl. 1, and imposes on him the duty to 'take Care that the Laws be faithfully executed' Art. II, § 3. It makes him the Commander in Chief of the Army and Navy, Art. II, §. cl. 1." _Quirin_, 317 U.S. at 26. The President, as Commander in Chief has "the power to wage war" which Congress has declared, "and to carry into effect all laws passed by Congress for the conduct of war and for the government and regulation of the Armed Forces, and all laws defining and punishing offenses against the law of nations, including those which pertain to the conduct of war." _Id_.

Military commissions derive their authority from these provisions of the Constitution as well as statutes, military usage, and the common law of war. _Quirin_, 317 U.S. at 26-28, 30, 34; Winthrop, _Military Law and Precedents_ at 831 (2d ed. 1920) (1920 Winthrop). Military tribunals have existed since the Revolutionary War, and Congress has long recognized the "'military commission'... as an appropriate tribunal for the trial and punishment of offenses against the law of war not ordinarily tried by courts-martial." _Quirin_, 317 U.S. at 26-27 (citing Articles of War 12, 15); _id_. at 42 n. 14 (listing revolutionary war military commissions). The Uniform Code of Military Justice, enacted in 1950, which provides rules for the government of the armed forces, also acknowledges the jurisdiction of the "military commission" for trial and punishment of "offenders or offenses" as provided "by statute or by the law of war." _See_ 10 U.S.C. §§ 821, 836, UCMJ, Act of May 5, 1950, ch. 169, 64 Stat. 107, 115, 120, 149 (quoted in _Hamdan_, 548 U.S. at 592-93, cited at 652 (Kennedy, Souter, Ginsburg, and Breyer, JJ., concurring in part)).

Colonel Winthrop explained the genesis of military commissions stating, "[I]n our military law, the distinctive name of military commission has been adopted for the exclusively war-court, which... is essentially a distinct tribunal from the court-martial of the Articles of war." 1920 Winthrop 831. He continued:

[I]n general, it is those provisions of the Constitution which empower Congress to "declare war" and "raise armies," and which, in authorizing the initiation of war authorize the employment of all necessary and proper agencies for its due prosecution, from which this tribunal derives its original sanction. Its authority is thus the same as the authority for the making and waging of war and for the exercise of military government
and martial law. The commission is simply an instrumentality for the more efficient execution of the war powers vested in Congress and the power vested in the President as commander-in-chief in war.

Id. (emphasis in original). In *Hamdan*, the Supreme Court agreed that military commissions have historically been used by the United States in three circumstances, and that the situation relevant to the conflict with al Qaeda is "incident to the conduct of war" when there is a need "to seize and subject to disciplinary measures those enemies who . . . have violated the law of war . . . ."20

1. Military Commissions Act of 2006

The 2006 M.C.A. was developed and passed in direct response to the Supreme Court's decision in *Hamdan*.21 The stated "purpose" of the 2006 M.C.A. is to "establish[] procedures governing the use of military commissions to try alien unlawful enemy combatants"22 engaged in hostilities against the United States for violations of the law of war and other offenses triable by military commission." 10 U.S.C. § 948b(a). The 2006 M.C.A. proclaims, "[t]he provisions of this subchapter codify offenses that have traditionally been triable by military commissions. This chapter does not establish new crimes that did not exist before its enactment, but rather codifies those crimes for trial by military commission" and acknowledges the effect of codifying pre-existing offenses stating, "[b]ecause the provisions of this subchapter . . . are declarative of existing law, they do not preclude trial for crimes that occurred before the date of enactment of this chapter." 2006 M.C.A. § 950p.

---

20 *Hamdan*, 548 U.S. at 596, 607 (Stevens, Souter, Ginsburg, and Breyer, JJ., concurring) (quoting *Quirin*, 317 U.S. at 28-29); *id.* at 683 (Thomas, Scalia, and Alito, JJ., dissenting) (citing *Quirin*, 317 U.S. at 28-29). The other two circumstances are: (1) to "substitute[] for civilian courts at times and in places where martial law has been declared" and (2) "as part of a temporary military government over occupied enemy territory or territory regained from an enemy where civilian government cannot and does not function." *Hamdan*, 548 U.S. at 595-96 (Stevens, Souter, Ginsburg, and Breyer, JJ., concurring) (citations omitted)).

21 It was intended to establish "a comprehensive statutory structure for military commissions that would allow for the fair and effective prosecution of captured members of al Qaeda and other unlawful enemy combatants," and "provided[ed] definitions rooted in United States law for the standards of conduct prescribed by Common Article 3." Message from the President of the United States, Transmitting the 2006 M.C.A. (H. Doc. No. 109-133), Cong. Rec. H6273 (Sept. 6, 2006). The draft procedures resulted from extended deliberation between the executive branch and Congress, and the procedures tracked those applicable in courts-martial, except where "impracticable or inappropriate for the trial of unlawful enemy combatants captured in the midst of an ongoing armed conflict." *Id.*

22 See infra n. 57 (noting the term "unprivileged belligerent" replaced the 2006 M.C.A. term "unlawful enemy combatant" in the 2009 M.C.A. § 948a(7) as a more contemporary international law term).
The jurisdiction of military commissions convened under the 2006 M.C.A. is limited to: (1) alien\textsuperscript{23} unlawful enemy combatants (AUEC),\textsuperscript{24} and (2) "any offense made punishable by this chapter or the law of war." 2006 M.C.A. § 948d(a). The significance of these limits on the jurisdiction of a military commission convened under the 2006 M.C.A. to our resolution of the assigned error is difficult to overstate. These limits define both the type of person subject to trial by military commission convened under the 2006 M.C.A., an AUEC, and the offenses for which that person may be tried. In a broad sense, these two provisions define the personal or \textit{in personam} jurisdiction and are fundamental to the definition of subject matter jurisdiction of military commissions convened under the 2006 M.C.A.

2. Congressional Authority to Define and Punish Offenses Against the Law of Nations

The parties agree the constitutional authority "To define and punish Offences against the Law of Nations" (the "Define and Punish Clause") provides Congress a basis to establish a statutory framework, such as the 2006 M.C.A., for trying and punishing violations of the law of war. U.S. Const. art. I, § 8, cl. 10. In addition, the Government asserts that when Congress exercises its authority to "define and punish" violations of the law of war, in conjunction with the Executive and "especially in the context of an armed conflict where national security is at stake, its judgment is entitled to the greatest deference."\textsuperscript{25} In response, appellant avers that the "Supreme Court has consistently required a plain and unambiguous showing that a war crime was established under the laws of war" when the charged conduct occurred.\textsuperscript{26}

\textsuperscript{23} 2006 M.C.A. § 948a(3) ("The term ‘alien’ means a person who is not a citizen of the United States.").

\textsuperscript{24} 2006 M.C.A. § 948a(1) ("(A) The term ‘unlawful enemy combatant’ means—(i) a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qaeda, or associated forces); or (ii) a person who, before, on, or after the date of the enactment of the Military Commissions Act of 2006, has been determined to be an unlawful enemy combatant by a Combatant Status Review Tribunal or another competent tribunal established under the authority of the President or the Secretary of Defense.").

\textsuperscript{25} Brief for Appellee 30 (citations omitted); see also Ex parte Quirin, 317 U.S. 1, 26 (1942) (listing U.S. Constitution's provisions at p. 18). See also Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635–37 (1952) (Jackson, J., concurring; citations omitted, quoted infra at n. 29).

\textsuperscript{26} Reply Brief on Specified Issues for Appellant 5 (citing Hamdan, 548 U.S. at 602 (Stevens, Souter, Ginsburg, and Breyer, JJ., concurring); In re Yamashita, 327 U.S. 1, 17 (1946); Quirin, 317 U.S. at 36; United States v. Yousef, 327 F.3d 56, 106 (2d Cir. 2003) (emphasis added)), but see Hamdan, 548 U.S. at 690-91 (Thomas, Scalia, and Alito, JJ., dissenting) ("The plurality holds that where, as here, ‘neither the elements of the offense nor the range of permissible punishments is defined by statute or treaty, the precedent
Judicial review of the scope of Congressional authority to define and punish offenses against the law of nations is infrequent. In an 1887 decision, the Supreme Court upheld a federal statute criminalizing the counterfeiting of foreign government securities explaining that “the obligation of one nation to punish those who within its own jurisdiction counterfeit the money of another nation has long been recognized [under the law of nations].” United States v. Arjona, 120 U.S. 479, 484 (1887). The Court went on to reason that “[w]hether the offense as defined is an offense against the law of nations depends on the thing done, not on any declaration to that effect by Congress.” Id. at 488. In Arjona, the Supreme Court did not address the scope of Congress’ discretion or what, if any deference, Courts should show a determination that a particular act constitutes an offense under the law of nations.

In 1820, the Supreme Court addressed Congressional authority in Article I, § 8, cl. 10, “[t]o define and punish Piracies and Felonies committed on the high seas,” the same clause containing the separate congressional power, “[t]o define and punish . . . Offenses against the Law of Nations.” United States v. Furlong, 18 U.S. 184, 198 (1820). The Court found a lack of nexus to the United States where Furlong, his victim, and the ship where the murder occurred were all British, and the Court concluded Congress had exceeded the scope of its constitutional authority by declaring “murder [at sea] to be piracy.” Id. at 195.

Furlong, a British subject, had engaged in an act of piracy against a British vessel, and while aboard that vessel killed another British subject. Id. at 195. He was tried and convicted by a U.S. court under a 1790 law criminalizing piracy to include the offense of murder. Id. at 193. The Supreme Court reasoned:

[t]hese are things so essentially different in their nature, that not even the omnipotence of legislative power can confound or identify them . . . . If by calling murder piracy, it might assert jurisdiction over that offence committed by a foreigner in a foreign vessel, what offence might not be brought within their power by the same device?

Id. at 198. We glean from Furlong that the Supreme Court recognized “the province and duty of the judicial department . . . to say what the law is” includes review of the Congressional exercise of authority “[t]o define and punish Piracies and Felonies committed on the high seas.” Marbury v. Madison, 5 U.S. 137, 177 (1803); U.S. Const., art. I, § 8, cl. 10.

[establishing whether an offense is triable by military commission] must be plain and unambiguous.” Ante, at 602. . . . [T]he actions of military commissions are ‘not to be set aside by the courts without the clear conviction that they are’ unlawful, 317 U.S., at 25 (emphasis added). It is also contrary to Yamashita, which recognized the legitimacy of that military commission notwithstanding a substantial disagreement pertaining to whether Yamashita had been charged with a violation of the law of war.”).
The outer boundaries of Congress’ discretion to “define and punish . . . Offences against the Law of Nations” and to make such conduct punishable by military commissions remain an open question.²⁷ An 1865 Attorney General Opinion suggests Congressional authority to “define” such offenses is limited:

To define is to give the limits or precise meaning of a word or thing [already] in being; to make is to call into being . . . Congress has the power to define, not to make, the laws of nations . . . Hence Congress may define those laws [and] may modify [those laws] on some points of indifference.²⁸

On the other hand, there is substantial authority supporting the Government’s position that “greatest deference” is due Congress’ determination that the offenses of which appellant stands convicted constitute offenses under the law of nations; particularly where that determination directly implicates both national security interests in an ongoing armed conflict and foreign affairs, including interpretation of treaty obligations and customary international law.²⁹

Nonetheless, we are not persuaded by the Government’s suggestion that Congress’ power to “define and punish . . . Offences against the Law of Nations,” U.S. Const., art. I, § 8, cl. 10, even when exercised in collaboration with the President in a time of armed conflict, includes the power to make conduct punishable by military commission without any reference to

---


²⁸ James Speed, Opinion of the Constitutional Power of the Military to Try and Execute the Assassins of the President, 11 Op. Atty. Gen. 297, 299 (1865) (emphasis in original)(internal quotation marks and citations omitted); see also Morison, supra n. 27, at 2 and n. 4 (citations omitted).

²⁹ Hamdan, 2011 WL 2923945 at *9-*14. See also Youngstown Sheet & Tube Co., 343 U.S. at 635-37 (Jackson, J., concurring; citations omitted)(“[The President’s authority] is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. In these circumstances, and in these only, may he be said (for what it may be worth) to personify the federal sovereignty. If his act is held unconstitutional under these circumstances, it usually means that the Federal Government as an undivided whole lacks power. [An action] executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it.”). Justice Jackson’s opinion in Youngstown has been frequently quoted in subsequent Supreme Court decisions, including Hamdan, 548 U.S. at 638, 680, as a clear expression of the Government’s power to regulate conduct in matters of national security. See also Holder v. Humanitarian Law Project, 561 U.S. ___, 130 S. Ct. 2705, 2727-29; 177 L. Ed. 2d 355 (2010) (noting the “weighty and sensitive interests”). See also Winthrop, Military Law and Precedents at 831 (2d ed. 1920)(1920 Winthrop).
international norms.\textsuperscript{30} It is emphatically the province and duty of a reviewing Court to “say ‘what the law is.’” Boumediene v. Bush, 553 U.S. 723, 128 S. Ct. 2229, 2259, 171 L. Ed. 2d 41, 77 (2008) (quoting Marbury, 5 U.S. at 177); see also Hamdan, 2011 WL 2923945 at *19 (citation omitted). We find this duty particularly compelling in the assessment of the constitutionality of a federal statute that by its plain language casts a wide, potentially global net of individual criminal liability, and we conclude this applies to our determination of whether Congress exceeded its constitutional authority by defining the subject conduct as punishable by military commission.\textsuperscript{31}

In making this determination, we will employ the “substantial showing” standard discussed in the Supreme Court’s Hamdan decision, aware that a standard more favorable to the Government may, as a matter of law, be applicable.\textsuperscript{32} Where Congress’ determination that certain acts constitute offenses

\textsuperscript{30} Brief for Appellee 18 (“So long as the political branches were justified in the exercise of their war powers, and the accused is a person properly subject to those powers, Congress and the President were within their authority to determine the jurisdiction of military commissions under the MCA because the offenses with which appellant was charged are offenses over which the MCA confers jurisdiction, appellant’s military commission properly exercised jurisdiction.”).

\textsuperscript{31} See Hamdan, 548 U.S. at 637 (Kennedy, Souter, Ginsburg, and Breyer, JJ., concurring); see generally Sanchez-Llamas v. Oregon, 548 U.S. 331, 353-54 (2006); see also Furlong, 18 U.S. at 198. Brief for Appellant 22 n. 6; Brief on Specified Issue for Appellant 24-25 and n. 13 (quoting U.S. Congress, Senate Committee on Armed Services, Military Commissions, 111th Cong., 1st sess., July 7, 2009 (Submitted statement of Jeh Johnson, General Counsel, Department of Defense) (“After careful study, the Administration has concluded that appellate courts may find that, ‘material support for terrorism’ . . . is not a traditional violation of the law of war. . . . We thus believe it would be best for material support to be removed from the list of offenses triable by military commission, which would fit better with the statute’s existing declarative statement.”); Id. (Prepared statement of David Kris, Assistant Attorney General) (“[T]here are serious questions as to whether material support for terrorism or terrorists groups is a traditional violation of the law of war. . . . our experts believe that there is a significant risk that appellate courts will ultimately conclude that material support for terrorism is not a traditional law of war offense[].”) (quoted in Elsea, CRS Report No. R40752, supra n. 16, at 10 n. 65). However, other witnesses recommended that Congress retain providing material support for terrorism as a law of war offense in the 2009 MCA. Sen. Comm. on Armed Services, Legal Issues Regarding Military Commissions and the Trial of Detainees for Violations of the Law of War, 111th Cong., 1st Sess. (S. Hrg. 111-190), 20, 105 (July 7, 2009). H.R. Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the Comm. on Jud., Proposals for Reform of the Military Commissions System, 111th Cong., 1st Sess., H.R. Doc 111-26 at 109, 121-23 (July 30, 2009). See also Hamdan, 2011 WL 2923945 at *16 n. 34, *34 n. 137 (listing citations to legislative history regarding whether the offense of providing material support to terrorism is part of the existing law of war); Report of Special Rapporteur Martin Scheinin on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Council, UN Doc. A/HRC/6/17/Add.3 (Nov. 22, 2007) 12 at ¶ 20 (“[T]he offences listed in [the 2006 M.C.A.] of (terrorism, providing material support for terrorism . . . and conspiracy) go beyond offences under the laws of war.”).

\textsuperscript{32} Hamdan 548 U.S. at 603 (Stevens, Souter, Ginsburg, and Breyer, JJ, concurring) (“At a minimum, the Government must make a substantial showing that the crime for which it seeks
under the law of nations is consistent with international norms, we also conclude that the specific statutory scheme employed by Congress to include the name of the offense, the elements of that offense, the forum by which that offense is punishable, and the applicable rules/procedures, is due great deference.\footnote{See generally Hamdan 548 U.S. at 603, 611 (Stevens, Souter, Ginsburg, and Breyer, JJ, concurring) id. at 702 (Thomas, Scalia, and Alito, JJ, dissenting). See Quirin, 317 U.S. at 25 ("the detention and trial of petitioners -- ordered by the President in the declared exercise of his powers as Commander in Chief of the Army in time of war and of grave public danger -- are not to be set aside by the courts without the clear conviction that they are in conflict with the Constitution or laws of Congress constitutionally enacted"); Cf. Furlong, supra p. 22.}

When incorporating existing offenses against the law of nations into American jurisprudence, it is well within Congress’ grant of authority under the Define and Punish Clause to define the specific elements of an offense in the context of the American legal system. See Hamdan, 2011 WL 2923945 at *17 and n. 40, *47 (citations omitted). This is particularly so when, as in the present instance, the executive and legislative branches act together and “weighty interests of national security and foreign affairs” are the basis for the legislative act. See supra n. 29. We begin our analysis by addressing the law of nations, the law of armed conflict, and their applicability in a non-international armed conflict.

3. The Law of Nations

When the U.S. Constitution was adopted, “the law of nations was understood” to be “a branch of natural law, deducible by reason, . . . obligatory on all nations,” and according to “Blackstone and Lord Mansfield, . . .

More recently, the law of nations or international law is defined as “rules and principles of general application dealing with the conduct of States and of international organizations and with their relations inter se, as well as some of their relations with persons, natural or juridical.” Restatement (Third) of Foreign Relations Law of the United States, § 101 (1987). This modern definition reflects the integration of humanitarian law, or perhaps more succinctly individual human rights, into the evolving body of law previously primarily related to relations among nation states with almost exclusive focus on state sovereignty.


The horrors of World War II produced a host of developments in international law, among the most significant was crystallization of the principle that violation of certain international norms, even on behalf of a nation state, could give rise to individual criminal responsibility. The emergence of this principle was primarily driven by the need for effective means of enforcement. The International Military Tribunal at Nuremberg reasoned, "[c]rimes against international law are committed by men, not by abstract entities, and only by punishing individuals who commit such crimes can the provisions of international law be enforced."\textsuperscript{36}

The sovereignty of states over their territory and nationals, the protection of "succeeding generations from the scourge of war," and the maintenance of "international peace" and security remain fundamental tenets of international law. Preamble and Article 1, United Nations Charter. The generally accepted sources of international law include:

a. international conventions establishing rules expressly recognized by the contesting states;

b. international custom, as evidence of a general practice accepted as law;

c. the general principles of law recognized by civilized nations;

d. . . . judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.\textsuperscript{37}

4. The Law of Armed Conflict

International law's traditional function of regulating relations between and among states is at the apex of importance when those relations degenerate

\textsuperscript{36} 1 Trials of the Major War Criminals Before the International Military Tribunal at 223 (1947). The 42-volume record, known as the "The Blue Series," of the Trial of the Major War Criminals before the IMT at Nuremberg, Nov. 14, 1945 to Oct. 1, 1946, is cited here as T.M.W.C. These volumes are available at http://www.loc.gov/rr/frd/Military_Law/NT_major-war-criminals.html.

\textsuperscript{37} Statute of the International Court of Justice (ICJ Statute), art. 38 (June 26, 1945), 59 Stat. 1055, 1060. See also Khulumani v. Barclay National Bank Ltd., 304 F.3d 254, 267 (2d Cir. 2007) (citation omitted); United States v. Hamdan, 2011 WL 2923945 at *10 (listing six sources of international law) (citing 11 Trials of War Criminals Before the Nuremberg Military Tribunals Under Control Council Law No. 10 at 1235 (1950)). Restatement (Third) of Foreign Relations Law § 102 (1987) ("(2) Customary international law results from a general and consistent practice of states followed by them from a sense of legal obligation. . . . (4) General principles common to the major legal systems, even if not incorporated or reflected in customary law or international agreement, may be invoked as supplementary rules of international law where appropriate.").
into armed conflict. Indeed, the regulation of armed conflict has long been recognized as essential to the preservation of civilization. The corpus of international norms that regulate the conduct of hostilities and that provide protection for persons not taking part, or no longer taking part, in hostilities is known as the law of armed conflict, \(^{38}\) is one of the oldest subject areas of international law. It is the “customary and treaty law applicable to the conduct of warfare . . . and to relationships between belligerents . . .” and “requires that belligerents refrain from employing any kind or degree of violence which is not actually necessary for military purposes and that they conduct hostilities with regard for the principles of humanity and chivalry.” Dep’t. of the Army, Field Manual 27-10, The Law of Land Warfare (1956) (1956 FM 27-10), ¶¶ 1, 3. See also Quirin, 317 U.S. at 29 (the law of war was not codified or bound by statute).

In his influential 1886 treatise, Colonel William Winthrop explained the laws or customs of war as:

[T]he rules and principles, almost wholly unwritten, which regulate the intercourse and acts of individuals during the carrying on of war between hostile nations or peoples. While properly observed by military commanders in the field, they may often also enter into the question of the due administration of justice by military courts in cases of persons charged with offences growing out of the state of war. Such laws and customs would especially be taken into consideration by military commissions in passing upon offences in violation of the laws of war.


Since Colonel Winthrop’s 1886 treatise, the number of conventions and treaties applicable in armed conflict has increased significantly. Most conventions addressing the law of armed conflict fall within two broad categories, “Hague Law” or “Geneva Law.” \(^{39}\) Hague law primarily addresses

\(^{38}\) Also known as the law of war or international humanitarian law, these phrases will be used synonymously throughout this opinion; see e.g., Manooher Mofidi & Amy E. Eckert, “Unlawful Combatants” or “Prisoners of War”: The Law and Politics of Labels, 36 Cornell Intl. L.J. 59, 61 (2003)(“International humanitarian law” is, broadly, that branch of public international law that seeks to moderate the conduct of armed conflict and mitigate the suffering it causes. It is predicated upon ideas . . . namely, that methods and means of warfare are subject to legal and ethical limitations, and that the victims of armed conflict are entitled to humanitarian care and protection.” (citation omitted)).

\(^{39}\) See generally Hague Convention IV (Hague IV) Respecting the Laws and Customs of War on Land (Oct. 18, 1907), 36 Stat. 2277; Hague Convention IX (Hague IX), Concerning Bombardment by Naval Forces in Time of War, (Oct. 18, 1907), 36 Stat. 2314; Hague Convention V (Hague V), Respecting the Rights and Duties of Neutrals Powers and Persons in Case of War on Land (Oct. 18, 1907); GCI to GCIV, supra n. 6. International Humanitarian Law includes two additional treaties with widespread adoption. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of
restraints on the conduct of hostilities, including the outright prohibition of certain means and methods of warfare. Richard D. Rosen, Targeting Enemy Forces in the War on Terror: Preserving Civilian Immunity, 42 Vand. J. Transnatl. L. 683, 692 and n. 41 (2009) (citations omitted). Geneva law primarily focuses on the “treatment of civilians and combatants rendered hors de combat who fall into a belligerent’s hands.” Id. at 709 (citations omitted). The United Nations Charter, the “Martens Clause,”40 and other treaties and conventions also factor into the law of armed conflict including defining who


40 The Martens Clause forms a part of the laws of armed conflict: “Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.” The Martens Clause first appeared in the preamble to the 1899 Hague Convention II (Hague II) with respect to the laws and customs of war on land, and is restated in GCI-IV and API and APII, see supra nn. 6, 39. See Rupert Ticehurst, The Martens Clause and the Laws of Armed Conflict, International Review of the Red Cross No. 317, at 125-34 (1997) (citing Preamble, Hague IV, supra n. 39; the four 1949 Geneva Conventions for the protection of war victims, supra n. 6 (GCI: art. 63; GCII: art. 62; GCIII: art. 142; GCIV: art. 158), op. cit., pp. 169-337; API, art. 1(2), op. cit., p. 390, and APII, Preamble, op. cit., p. 449; 1980 Weapons Convention, Preamble, op. cit., p. 473), http://www.loc.gov/rr/frd/Military_Law/pdf/RC_Mar-Apr1997.pdf.
may lawfully engage in armed conflict and when resort to armed force is lawful under international law. Laws or customs of armed conflict are grounded in four key principles: (1) distinction;\(^{41}\) (2) military necessity;\(^{42}\) (3) proportionality;\(^{43}\) and (4) humanity.\(^{44}\) These four principles are the cornerstones for the lawful conduct of armed conflict, and more relevant to our inquiry, the deviation from which may provide the basis for individual criminal responsibility for violation of the laws and customs of war.

a. Combatants — Lawful and Unlawful

While the aforementioned principles impose restraints on the conduct of hostilities, the "combatants' privilege" is a fundamental rule of the law of armed conflict. The "privilege of combatant immunity" is limited to "lawful combatants" and "the quid pro quo for attaining such immunity must be that combatants distinguish themselves from the civilian population - that is,

\(^{41}\) See Chapter 5.3.2, U.S. Dep't of the Navy, Naval Warfare Publication 1-14M/U.S. Marine Corps MCPW 5-12.1, The Commander's Handbook on the Law of Naval Operations (July 2007) [hereinafter NWP 1-14M] ("The principle of distinction is concerned with distinguishing combatants from civilians and military objects from civilian objects so as to minimize damage to civilians and civilian objects."); see also API, art. 48, see supra n. 39 ("Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."); Daphne Richemond, Reexamining the Law of War: Transnational Terrorist Organizations and the Use of Force, 56 Cath. U.L. Rev. 1001, 1018 and n. 81 (2007) (citing Francisco de Vitoria, De Indis et de Ivo Belli Reflectiones (Ernest Nys ed., John Pawley Bate trans., 1917) (1532), reprinted in 1 The Classics of International Law at 171 (James Brown Scott ed., 1917) ("we may not turn our sword against those who do us no harm, the killing of innocent being forbidden by natural law.").

\(^{42}\) Article 23(g), Annex to Hague IV ("it is especially forbidden . . . . To destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war"); See also Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (May 15, 2011) (military necessity — The principle whereby a belligerent has the right to apply any measures which are required to bring about the successful conclusion of a military operation and which are not forbidden by the laws of war; Dep't of the Army, Field Manual 27-10, The Law of Land Warfare, (1956) (1956 FM 27-10) at ¶ 3; NWP 1-14M, supra n. 41, at 5.3.1.

\(^{43}\) See NWP 1-14M, supra n. 41, at 5.3.3, ("The principle of proportionality requires the commander to conduct a balancing test to determine if the incidental injury, including death to civilians and damage to civilian objects, is excessive in relation to the concrete and direct military advantage expected to be gained."); API, art. 51(5)(b), supra n. 39 ("An attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" violates the principle of proportionality.").

‘persons entitled to immunity for pre-capture war-like acts must have made themselves legitimate targets while performing those acts.’” Rosen, supra n. 39, at 770 (citation omitted). Lawful combatants enjoy “combatant immunity” for their pre-capture acts of warfare, including the targeting, wounding, or killing of other human beings, provided those actions were performed in the context of ongoing hostilities against lawful military targets, and were not in violation of the law of war.45 Article 4, of GCIII, supra n. 6, makes it clear that lawful combatants will generally only include the regular armed forces of a party to the conflict, including “members of militias or volunteer corps forming part of such armed forces” and members of other militia, volunteer corps, and organized resistance movements belonging to a State party to the conflict so long as they fulfill the following four conditions that are also included in the 2006 M.C.A. § 948a(2) infra at n. 53:

1. They are under the command of an individual who is responsible for their subordinates;

2. They wear a fixed distinctive sign or symbol recognizable at a distance;

3. They carry their arms openly; and

4. They conduct their operations in accordance with the laws and customs of war.

The law of armed conflict regulates the means by which armed force is employed, to include the intentional killing of other human beings. Lawful combatants are immunized from prosecution for the act of killing, so long as the fundamental principles of the law of armed conflict are not violated.

“Lawful enemy combatants [have] ... combatant immunity and [enjoy] ... the protections of the Geneva Conventions if wounded or sick, and while being held as prisoners of war (POWs).” United States v. Khadr, 717 F. Supp. 2d 1215, 1221 (USCMCR 2007) (citations omitted). Lawful enemy combatants, who are being tried for offenses that violate the law of war or for their “post-capture offenses committed while they are POWs, are entitled to be tried by the same courts, and in accordance with the same procedures, that the detaining power would utilize to try members of its own armed forces (i.e., by court-martial for lawful enemy combatants held by the United States).” Id. (citing GCIII, supra n. 6, arts. 84, 87 and 102.).

---

“By universal agreement and practice, the law of war draws a distinction between the armed forces and the peaceful populations of belligerent nations and also between those who are lawful and unlawful combatants.” *Quirin*, 317 U.S. at 30-31 and n. 7 (citing Hague Convention No. IV (Oct. 18, 1907), 36 Stat. 2295, and Annex I to Hague Convention No. IV; other citations omitted). This determination of “lawful” or “unlawful” combatant status is far more than simply a matter of semantics. Unlawful combatants are not entitled to “combatant immunity” or the privileges generally afforded lawful combatants who become POWs. “Unlawful combatants are likewise subject to capture and detention, but in addition they are subject to trial and punishment by military tribunals for acts which render their belligerency unlawful.” *Id.* at 31; see also *United States v. Lindh*, 212 F. Supp. 2d 541, 554 (E.D. Va. 2002).

Prior to implementation of Common Article 3, irregular bands of men carrying on irregular wars not in compliance with the law of armed conflict were under the common law of war upon capture subject to a punishment of death, often without trial. [46] “[S]entences and executions without a proper trial were common practice” in many nations prior to 1949, and they were “nevertheless shocking to the civilized” drafters of GCII-GCIV. [47] Common Article 3 prohibits “the passing of sentences ... without previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples.” [48]

[46] David Glazier, *The Laws of War: Past, Present, and Future: Precedents Lost: The Neglected History of the Military Commission*, 46 Va. J. Intl. L. 5, 36 (2005) (“[I]t was 'a universal right of war, not to give quarter to an enemy that puts to death all who fall into his hands.' [General Winfield Scott, during the Mexican War in 1847,] could have had the outlaws[, who attacked stragglers from the American Army,] shot on the spot. As a logical result, any procedural due process provided exceeded international requirements.” (citations omitted)). See also Louis Fisher, Military Tribunals: *Military Tribunals: Historical Patterns and Lessons* at 19, (CRS Report Order Code No. RL32458, July 9, 2004) (quoting *The War of the Rebellion: A Compilation of the Official Records of the Union and Confederate Armies*, ser. II, vol. 1 242-43 (1894) (“It was a well-established principle, said General Halleck, that 'insurgents and marauding, predatory and guerrilla bands are not entitled' to an exemption from military tribunals. These men are 'by the laws of war regarded as no more nor less than murderers, robbers and thieves.'”).


[48] Common Article 3(1)(d). See Pictet, supra n. 47, at 54 (“All civilized nations surround the administration of justice with safeguards aimed at eliminating the possibility of errors. The Convention has rightly proclaimed that it is essential to do this even in time of war. We must be very clear about one point: it is only ‘summary’ justice which it is intended to prohibit. No sort of immunity is given to anyone under this provision. There is nothing in it to prevent a person presumed to be guilty from being arrested and so placed in a position where he can do no further harm; and it leaves intact the right of the State to prosecute, sentence and punish according to the law.”).
Although international conventions and treaties primarily address international armed conflict or “conflict between nations,” in *Hamdan*, the Supreme Court concluded that “at least” Common Article 3 of the Geneva Conventions (so called because it appeared in all four conventions) applies to the United States’ conflict with Al Qaeda. *Hamdan* at 548 U.S. at 629-30. The Court reasoned:

in a “conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party[49] to the conflict shall be bound to apply, as a minimum,” certain provisions protecting “[p]ersons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by . . . detention.”

*Id.* (citing GCIII, art. 3, ¶ 1(d), 6 U.S.T. at 3320). In *Hamdan*, noncompliance with the requirement that “judgment [be] pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples,” *id.* at 630, 632 (citing GCIII, art. 3, ¶ 1(d), 6 U.S.T. at 3320), provided one of the two primary bases for the Supreme Court’s conclusion that the military commission convened under Military Commission Order No. 1, lacked the authority to try Hamdan. *Id.* at 632-33.

Common Article 3, applicable to the United States’ conflict with al Qaeda, reflects elementary considerations of humanity, “provides a rudimentary framework of minimum standards[,] and does not contain much detail.” Customary International Humanitarian Law (IHL), International Committee of the Red Cross (ICRC), 2005, vol. I at Intro. XXXV. Common Article 3 was adopted to provide minimum humanitarian standards applicable in internal armed conflict, including prohibition of “sentences and executions without previous trial” or “summary justice.” GCIII, *supra* n. 6. Less than one typed page in length, Common Article 3 declares in GCIII:

In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions:

(1) Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed ‘hors de combat’ . . . shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria. To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons: (a) violence to life and person,

---

[49] The term “Party” here has the broadest possible meaning; a Party need neither be a signatory of the Convention nor “even represent a legal entity capable of undertaking international obligations.” GCIII Commentary 37.
particular murder of all kinds, mutilation, cruel treatment and torture; (b) taking of hostages; (c) outrages upon personal dignity, in particular humiliating and degrading treatment; (d) the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.

Common Article 3 is supplemented by APII.\textsuperscript{50} APII is comprised of 28 articles, including “fundamental guarantees” prohibiting:

at any time and in any place whatsoever: (a) violence to the life, health and physical or mental well-being of persons, in particular murder as well as cruel treatment such as torture, mutilation or any form of corporal punishment . . . (c) taking of hostages . . . (d) acts of terrorism; [and] (h) threats to commit any or the foregoing acts.

APII, art. 4, ¶¶ 1-2. “Protection of the civilian population” is of fundamental import:

1. The civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations. \textit{To give effect to this protection, the following rules shall be observed in all circumstances.} 2. \textit{The civilian population} as such, as well as individual civilians, shall not be the object of attack. \textit{Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.} 3. Civilians shall enjoy the protection afforded by this Part, unless and for such time as they take a direct part in hostilities.

APII, art. 13, \textit{supra} n. 39 (emphasis added).

Suffice it to say there is no statute, treaty, or other international agreement which exhaustively details all offenses or conduct violative of the laws or customs of war. However, the “fundamental guarantees” of treaties applicable “at any time and in any place whatsoever” including conflicts not of an international character, explicitly prohibit: murder, the intentional targeting

\textsuperscript{50} The White House, Office of the Press Secretary, Fact Sheet: \textit{New Actions on Guantánamo and Detainee Policy}, Mar. 7, 2011 (“Because of the vital importance of the rule of law to the effectiveness and legitimacy of our national security policy, the Administration is announcing our support for . . . [APII] . . . [This protocol] contains . . . fair trial guarantees that apply in the context of non-international armed conflicts, was originally submitted to the Senate for approval by President Reagan in 1987. The Administration urges the Senate to act as soon as practicable on this Protocol[.] An extensive interagency review concluded that United States military practice is already consistent with the Protocol’s provisions”)(emphasis added); see also President Reagan, Message to the Senate Transmitting APII, Jan. 29, 1987, \url{http://www.loc.gov/rr/frd/Military_Law/pdf/protocol-II-100-2.pdf}. See also \textit{supra} n. 39.
of civilians, "acts of terrorism," and "acts or threats of violence the primary purpose of which is to spread terror among the civilian population" as specifically alleged or directly implicated here. See Discussion of Common Article 3 and APII at pp. 33-34, supra n. 39. These fundamental guarantees and prohibitions are central to determining whether appellant was lawfully tried and punished by military commission. Although Common Article 3 does not specifically adopt individual criminal liability for its violation, violations of Common Article 3 are considered domestically and internationally as crimes or war crimes.51

The Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia (ICTY), an ad hoc tribunal established by the United Nations in 1993 to address varying atrocities that took place during the conflicts in the Balkans in the 1990s, addressed this very issue. In Tadić, the Appeals Chamber found that certain norms of international armed conflict have evolved through customary law and now apply during non-international armed conflict as well. Prosecutor v. Tadić, Case No. IT-94-1-AR72, Jurisdiction Appeal, ¶¶ 67-71 (Oct. 2, 1995). Specifically:

that an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved.

Tadić, IT-94-1-AR72 at ¶ 70. Although we are not bound by the ICTY Appeals Chamber's decision in Tadić, the principles embodied in Tadić reveal that conduct during armed conflict that breaches fundamental principles or values may provide the basis for individual criminal liability for violation of the common law of war.

Fundamental laws applicable in any armed conflict, regardless of type, and relevant here include:

(1) Lawful combatants enjoy combatant immunity for pre-capture acts of warfare performed in the context of ongoing hostilities against lawful military targets. To qualify as a lawful combatant an individual must satisfy the conditions specified in the 2006 M.C.A. § 948a(2) infra at n. 53 and listed supra p. 31.

(2) The law of armed conflict prohibits the intentional targeting of civilians and “[a]cts or threats of violence the primary purpose of which is to spread terror among the civilian population.”

In stark contrast to these fundamental humanitarian principles and in direct contravention of the explicit prohibitions articulated in Common Article 3 and APII are the words posited by bin Laden, and the actions of al Qaeda, both before and after that edict. In February 1998, bin Laden, ostensibly speaking for “The International Islamic Front for Jihad against the Jews and Crusader,” announced a “legal fatwa” to “[o]ur Muslim Nation.” Prosecution Ex. 22. In that announcement, he declared that:

The judgement to kill Americans and their allies, both civilian and military is the individual duty of every Muslim able to do so . . . We in the name of God, call on every Muslim who believes in God and desires to be rewarded, to follow God’s order to kill Americans and plunder their wealth wherever and whenever they find it.

Prosecution Ex. 22 at 2.

On May 28, 1998, bin Laden was interviewed by ABC News and reiterated that “[w]e do not differentiate between those dressed in military uniforms and civilians, they are all targets in this fatwah.” Prosecution Ex. 24 at 2. On May 29, 1998, bin Laden issued a declaration called “The Nuclear Bomb of Islam” which included the statement, “it is the duty of Muslims to prepare as much force as possible to terrorize the enemies of God.”

52 Henckaerts, supra n. 15, vol. 1 at 3-10 (citing primarily API, art. 51(2); GCIV, art. 33; and APII, arts. 4(2)(d), 13(2)). APII, art. 13 is quoted starting at p. 34. See also supra n. 39.
With this foundational framework we turn to the statutory elements of the three offenses of which appellant stands convicted. We will discuss the elements common to all three offenses, and then discuss each offense individually.

(1) Alien Unlawful Enemy Combatant (AUEC) – Common Element 1

The term AUEC is fundamental to determining both persons subject to trial by military commission, and the subject matter jurisdiction of military commissions convened under the 2006 M.C.A. Each specification states that appellant was an “alien unlawful enemy combatant” and alleges a direct nexus to al Qaeda. See Charges, infra pp. 48, 86, 97. The statute, as written and as applied at trial, confirms the essential jurisdictional function of the AUEC determination.

The 2006 M.C.A. explicitly limits jurisdiction over persons subject to trial by military commission to AUECs and defines an AUEC as a person who: (1) was not a citizen of the United States, (2) was not a “lawful combatant,” and (3) was an “unlawful enemy combatant,” see supra n. 24 (quoting 2006 M.C.A § 948a(1)).

At trial, the military commission judge made a threshold determination that appellant was an “unlawful enemy combatant,” for the limited purpose of establishing jurisdiction, as that term is defined in the 2006 M.C.A. § 948a(1). Tr. 836-37, 873. The military commission judge’s ruling, by a preponderance of the evidence, was consistent with his duty to rule on “interlocutory questions and all questions of law” and practice in courts-martial. The military

53 2006 M.C.A § 948a(2) ("The term 'lawful enemy combatant' means a person who is—
(A) a member of the regular forces of a State party engaged in hostilities against the United States; (B) a member of a militia, volunteer corps, or organized resistance movement belonging to a State party engaged in such hostilities, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the law of war; or (C) a member of a regular armed force who professes allegiance to a government engaged in such hostilities, but not recognized by the United States.

54 The military commission judge’s findings reflect a potential error and a potential omission. First, the military commission judge did not enter a finding that appellant was an “alien” as defined in the 2006 M.C.A. § 948a. Instead, trial defense counsel stipulated that appellant was an alien, and the military commission judge accepted that stipulation through judicial notice. The military commission judge also took judicial notice of a “certificate of nonexistence of records” that appellant “is or has ever been a lawful resident of the United States.” Tr. 87-88, 298-99, 837, 873. Likewise, he did not explicitly find that appellant was not a “lawful combatant,” as that term is defined in the 2006 M.C.A. § 948a(1). See supra n. 24. Though not challenged at trial or on appeal, assuming arguendo it was error, we conclude that any such error did not materially prejudice the substantial rights of appellant. 2009 M.C.A. § 950a(a).

55 2007 M.M.C., Part II, R.M.C. 801(a)(4) (the military commission judge “[r]ule[s] on all interlocutory questions and all questions of law raised during the military commissions”);
commission judge also required the fact finders to determine, based upon legal and competent evidence, "beyond a reasonable doubt, [whether appellant] was an alien unlawful enemy combatant and [whether] the alleged conduct occurred in the context of and was associated with an armed conflict." Tr. 843-44.

Based upon the record before us, making allowances for not having personally observed the witnesses, we agree with the military commission judge and the members that appellant was an AUEC, as defined by the 2006 M.C.A., and conclude that the military commission properly exercised jurisdiction over him. We base this conclusion on our findings, beyond any reasonable doubt that: (1) appellant was a member of al Qaeda during the charged time frame as evidenced by his admissions and other corroborating evidence; (2) appellant was a citizen of Yemen, and that he was neither a citizen nor resident of the United States; and (3) that appellant was not a lawful combatant, as that term is defined in 2006 M.C.A. § 948a(2). See supra n. 53.

The specification of each charge explicitly stated that appellant was an AUEC and alleged a direct nexus to al Qaeda. The 2006 M.C.A. defines "unlawful enemy combatant" as "a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qaeda, or associated forces)." 2006 M.C.A. § 948a(1), supra n. 24. This definition implicitly reflects that membership in al Qaeda renders an individual an unlawful enemy combatant potentially punishable by military commission if that person is also an "alien" and not otherwise a "lawful combatant." This implication was made explicit in the 2009 M.C.A. where an "unprivileged enemy belligerent," "means an individual (other than a privileged belligerent) who – (C) was a part of al Qaeda at the time of the charged offense under this chapter." 2009 M.C.A. § 948a(7)(C). See infra n. 58.

The military commission judge applied the 2006 M.C.A. precisely in that manner. He instructed the members that the AUEC determination was an element "common to all the offenses," and further instructed that "the government must prove to you beyond a reasonable doubt that [appellant] was an AUEC, defining each key term in accordance with the statute."

Id. at R.M.C. 801(e)(2) ("Questions of fact in an interlocutory question shall be determined by a preponderance of the evidence, unless otherwise stated in this Manual.").

56 See MCM (2008), Part II, R.C.M. 801(a)(4) and Discussion, R.C.M. 801(e)(4) and Discussion, App. 21-42 to 21-44.

57 The record, including appellant’s pretrial admissions, establish beyond any reasonable doubt that he was a citizen of Yemen, and there was no evidence presented supporting a finding that appellant was a lawful combatant. Moreover, the members, based upon the military commission judge’s instructions concluded beyond a reasonable doubt that appellant was an alien unlawful enemy combatant (AUEC) and not a lawful combatant as defined in the 2006 M.C.A. § 948a(2). Tr. 843-44, 846, 859, 869, 916-17. See also supra nn. 23, 24, 53.
appellant's status as an AUEC was crucial to the military commission's exercise of jurisdiction over appellant and determination of his guilt.

(a) AUEC and the Law of Armed Conflict

Under the law of armed conflict, an AUEC is effectively synonymous with "unprivileged enemy belligerent," in other words a belligerent who is not entitled to "combatant immunity" or, upon capture, treatment as a prisoner of war. It is based upon the statutory language and findings required by the military commission judge and members. Congress' substitution of the phrase "unprivileged enemy belligerent" for "unlawful enemy combatant" in the 2009 M.C.A. further supports this proposition.\(^{58}\)

As previously discussed, "unlawful combatants are . . . subject to trial and punishment by military tribunals for acts which render their belligerency unlawful." Quirin, 317 U.S. at 30-31. The Supreme Court has long recognized that "men and bodies of men, who, without being lawful belligerents nevertheless commit hostile acts of any kind are not entitled to the privileges of prisoners of war if captured, and may be tried by military commission and punished by death or lesser punishment." Id. at 34 (citing 1940 Rules of Land Warfare promulgated by the War Department for the guidance of the Army, ¶ 351(internal quotation marks omitted). Clearly, both the plain language of the 2006 M.C.A., see supra n. 24, and Quirin use the word "unlawful" in contradistinction to the word "lawful" or "privileged." See supra n. 58.

(b) Irregular Warfare

At the time of the Civil War it was a well-established principle that guerilla-type bands were not exempt from military tribunals, and by the "laws of war" treated as murderers, robbers and thieves. Fisher, supra n. 46, at 19 (citation omitted). Early in the American Civil War then General-in-Chief of the U.S. Army, Major General (MG) H. W. Halleck posed several related questions to Dr. Francis Lieber, a noted law of war expert and future author of the Lieber Code, one of the first comprehensive lists of the laws of war.\(^{59}\) General Halleck noted:

\(^{58}\) Compare 2009 M.C.A. § 948a(7) with 2006 M.C.A. § 948a(1), supra n. 24. See also Hamdan, 2011 WL 2923945 at *18 n. 48 (citations omitted) (explaining why Congress changed the term from "unlawful combatant" to "unprivileged enemy belligerent").

\(^{59}\) Lieber was the lead author of Army General Orders 100 (1863) (G.O.100), which was subsequently styled the Lieber Code. See Francis Lieber, Instructions for the Government of Armies of the United States in the Field (Lieber's Instructions) 2 (1898). On April 24, 1863, President Abraham Lincoln approved G.O. 100, and directed its publication, "for the information of all concerned." Id. The Lieber Code represented one of the first comprehensive lists of the laws of war. Rosen, supra n. 39, at 695 ("The Lieber Code established the basis for later international conventions on the laws of war at Brussels in 1874 and at The Hague in 1899 and 1907.") (citation omitted)).
rebel authorities claim the right to send men, in the garb of peaceful citizens, to waylay and attack [Union] troops, to burn bridges and houses, and to destroy property and persons within [Union] lines. They demand that such persons be treated as ordinary belligerents, and that when captured they [be treated as prisoners of war]; they also threaten that if such persons be punished as marauders and spies, that they will retaliate by executing [Union] prisoners of war in their possession. I particularly request your views on these questions.


> [t]he position of armed parties loosely attached to the main body of the army, or altogether unconnected with it has rarely been taken up by writers on the law of war. . . . We find that self-constituted bands in the South, who destroy the cotton stored by their own neighbors, are styled in the journals of the North as well as those in the South, Guerillas: while in truth they are, according to the common law – not of war only, but that of every society – simply armed robbers, against whom every person is permitted, or is in duty bound, to use all means of defense at his disposal[.]


> [I]t is universally understood in this country . . . that a guerrilla party means an irregular band of armed men, carrying on an irregular war, not being able according to their character as a guerrilla party, to carry on what the law terms a regular war. The irregularity of the guerrilla party consists in its origin, for it is either self-constituted or constituted by the call of a single individual, not according to the general law of levy, conscription, or volunteering . . . and it is irregular as to the permanency of the band, which may be dismissed and called again together at any time. . . . Guerrilla parties . . . do not enjoy the full benefit of the laws of war. . . . The reasons for this are, that they are annoying and insidious, . . . [guerrilla parties] carry on petty war (guerrilla) chiefly by raids, extortion, destruction, and massacre, and . . . generally give [prisoners] no quarter[.]

*Id.* at 7-8, 18-19.

Nor can it be maintained in good faith . . . that . . . an armed prowler – (now frequently called a bushwhacker) shall be entitled to the protection
of the law of war, simply because he says he has taken up his gun in
defence of his country, or because . . . his chief has issued a proclamation
by which he calls upon the people to . . . commit homicides which every
civilized nation will consider murders. . . . The most disciplined soldiers
will execute on the spot an armed and murderous prowler found where he
could have no business as a peaceful citizen. . . . the so-called
bushwhacker, is a simple assassin, and will thus always be considered by
soldier and citizen . . . They unite the fourfold character of the spy, the
brigand, the assassin and the rebel, and cannot . . . expect to be treated as
a fair enemy of a regular war. They know what a hazardous career they
enter upon when they take up arms, and that, were the case reversed, they
would surely not grant the privilege of regular warfare to persons who
should thus rise in their rear.

*Id.* at 17, 20-21.

How far rules which have formed themselves in the course of time
between belligerents might be relaxed, with safety, . . . So much is
certain, that no army, no society, engaged in war, any more than a society
at peace, can allow unpunished assassination, robbery, and devastation,
without the deepest injury to itself and disastrous consequences[.]

*Id.* at 21-22.

This reasoning was repeated in Attorney General Speed's opinion
regarding trial by military commission of those charged with conspiring to
assassinate President Lincoln. He concluded that the act of:

unit[ing] with banditti, jayhawkers, guerillas, or any other unauthorized
raiders is a high offence against the laws of war; the offence is
complete when the band is organized or joined. The atrocities committed
by such a band do not constitute the offence, but make the reasons . . .
why such banditti are denounced by the laws of war.

James Speed, *Opinion of the Constitutional Power of the Military to Try and

Post World War II, before the International Military Tribunal at
Nuremburg, both the Chief French Prosecutor and Deputy Chief French
Prosecutor acknowledged that unlawful belligerents or "francs-tireurs could be
condemned to death[.]

---

60 5 T.M.W.C., *supra* n. 36, at 405 (Chief Prosecutor M. Francois de Menthon, French
Republic, stated to the IMT, "To be sure, the members of the Resistance rarely complied with
the conditions laid down by the Hague Conventions, which would qualify them to be
considered as regular combat forces; they could be sentenced to death as francs-tireurs and
executed. But they were assassinated without trial in most cases, often after having been
Germany under the authority of Control Council No. 10, known as the Nuremberg Military Tribunals (NMT) and considered international tribunals administering international law. In "The United States of America vs. Wilhelm List, et al." a U.S. Tribunal agreed with the contention of the defendant List, a former German Armed Forces Commander Southeast:

that the guerrilla fighters with which he contended were not lawful belligerents entitling them to prisoner of war status upon capture. [The Court is therefore] obliged to hold that such guerrillas were francs-tireurs who, upon capture, could be subjected to the death penalty. Consequently, no criminal responsibility attaches to the defendant List because of the execution of captured partisans in Yugoslavia and Greece.

11 T.W.C., supra n. 60, at 1269, see also id. at 529-30, 1244 (discussing necessity for compliance with the four requirements in the Annex to the Hague Convention, art. 1, at p. 31); 2006 M.C.A. § 948a(2), supra n. 53 (requirements for lawful combatant). The Tribunal also held that List’s deputy, Walter Kuntze, had “no criminal responsibility . . . because of the killing of captured members of the resistance forces, they being francs-tireurs subject to such punishment.” Id. at 1276.

(c) U.S. Army 1914 and 1956 Manuals

In 1914, the United States War Department “replaced General Orders No. 100 with an Army Field Manual entitled ‘The [Rules] of Land Warfare’ which, updated, is still in force.”61 The purpose of the 1914 Manual was to provide authoritative guidance to military personnel on customary and treaty law applicable to the conduct of warfare on land. 1914 Manual at 3, 11-13. The 1914 Manual ¶¶ 369, 371, and 373 permit prosecution as war criminals of individuals who engage in hostilities without qualifying as lawful combatants or privileged belligerents stating:

369. Hostilities committed by individuals not of armed forces.—Persons who take up arms and commit hostilities without having complied with the conditions prescribed for securing the privileges of belligerents,

terribly tortured.); 11 Trials of War Criminals Before the Nuremberg Military Tribunals under Control Council Law No. 10, at 388 (1951). An abbreviated official edition of Trials of War Criminals Before the Nuremberg Military Tribunals under Control Council Law No. 10 was published as 15 volumes, are abbreviated as T.W.C., and are known as “The Green Series.” The case number, name of lead defendant, popular name, and volume are listed at infra n. 85, http://www.loc.gov/rr/frd/Military_Law/NTs_war-criminals.html.

are, when captured by the enemy, liable to punishment for such hostile acts as war criminals.

371. Highway robbers and pirates of war.—Men, or squads of men, who commit hostilities, whether by fighting, or by inroads for destruction or plunder, or by raids of any kind, without commission, without being part and portion of the organized hostile army, and without sharing continuously in the war, but who do so with intermittently returns to their homes and avocations, or with the occasional assumption of the semblance of peaceful pursuits, divesting themselves of the character or appearance of soldiers—such men, or squads of men, are not [lawful combatants or privileged belligerents], and, therefore, if captured, are not entitled to the privileges of prisoners of war, but shall be treated summarily as highway robbers and pirates. [citing] G.O. 100, 1863, art. 82[, supra n. 59.]

373. Armed prowlers.—Armed prowlers, by whatever names they may be called, or persons of the enemy’s territory, who steal within the lines of the hostile army for the purpose of robbing, killing, or of destroying bridges, roads, or canals, or of robbing or destroying the mail, or of cutting the telegraph wires, are not entitled to the privileges of the prisoner of war. [citing] G.O. 100, 1863, art. 84[, supra n. 59.]

In 1942, the Supreme Court cited the 1914 and 1940 Rules of Land Warfare as the War Department’s guidance to the Army on war crimes. See Quirin, 317 U.S. at 33-34. In 1956, the U.S. Army updated the 1940 version of the Rules of Land warfare with Dep’t of the Army, Field Manual 27-10, The Law of Land Warfare (1956 FM 27-10). The 1956 FM 27-10 ¶¶ 502-504 listed grave breaches of the Geneva Conventions and a representative list of other war crimes. At ¶ 499 it defines “the term ‘war crime’” to be “the technical expression for a violation of the law of war by any person or persons, military or civilian. Every violation of the law of war is a war crime.” Like the 1914 Manual, the 1956 FM 27-10 permits prosecution of unlawful combatants or unprivileged belligerents as war criminals stating:

80. Individuals Not of Armed Forces Who Engage in Hostilities
Persons, such as gue[rillas and partisans, who take up arms and commit hostile acts without having complied with the conditions prescribed by the laws of war for recognition as belligerents (see [GCIII], art. 4; par. 61 herein), are, when captured by the injured party, not entitled to be treated as prisoners of war and may be tried and sentenced to execution or imprisonment.

81. Individuals Not of Armed Forces Who Commit Hostile Acts
Persons who, without having complied with the conditions prescribed by the laws of war for recognition as belligerents (see [GCIII], art. 4; par. 61 herein), commit hostile acts about or behind the lines of the enemy are not
to be treated as prisoners of war and may be tried and sentenced to execution or imprisonment. Such acts include, but are not limited to, sabotage, destruction of communications facilities, intentional misleading of troops by guides, liberation of prisoners of war, and other acts not falling within Articles 104 and 106 of the Uniform Code of Military Justice and Article 29 of the Hague Regulations.

The 1956 Field Manual provides for punishment of those who assist in illegal hostilities stating in ¶ 82 that persons culpable under ¶¶ 80 and 81 "who have attempted, committed, or conspired to commit hostile or belligerent acts are subject to the extreme penalty of death because of the danger inherent in their conduct. Lesser penalties may, however, be imposed."

(d) Terrorists

A former Legal Adviser, U.S. State Department, eloquently addressed the status of terrorists vis-à-vis privileged or lawful belligerency in the following statement:

Terrorists are belligerents who lack the entitlements of those legitimately engaged in combat. No colorable argument has been put forward that terrorists are entitled to any special status under the law of armed conflict - and certainly not to the status of prisoners of war under [GCIII]. As a group, terrorists willingly define and conduct themselves outside the coverage of Article 4 of the [GCIII]: They are neither members of the armed forces of a State Party nor members of a "regular" armed force. Even if generously considered, in the broadest sense, "irregulars" of some sort, they willfully and maliciously fail to distinguish themselves from the civilian population, as impliedly required by the four conditions laid down in the 1907 Hague Regulations and repeated in Article 4(A)(2) of the [GCIII]. In fact, the core aspect of terrorism is that its perpetrators fail on a systematic and willful basis to conduct "their operations in accordance with the laws and customs of war," as required by Article 4(A)(2)(d).

[A]rticle 4 . . . imposes a distinction between the legitimate and the illegitimate combatant - and while Article 4 expressly entitles the legitimate soldier to the [GCIII]'s protections, its real beneficiaries are the civilians who make up the mass of our societies.

* * *

Terrorism is, above all, the negation of law. More specifically, it is the negation of the fundamental humanitarian principles of the law of armed conflict. Whereas humanitarian law proscribes directing attacks against civilians as such, terrorism promotes it; and whereas a fundamental
purpose of *jus in bello* is the facilitation of order after a conflict, the aim of terrorism is the opposite - chaos clad in violence. . . . Application of the law of armed conflict, and in particular its bedrock principles of distinction and fundamental protections, serves humanitarian ends and ultimately reinforces the rules governing international behavior at all times, even in war. 62

(e) Conclusion

The 2006 M.C.A. definition of an AUEC is consistent with the meaning of an unprivileged belligerent under the common law of armed conflict. See supra n. 58. In the absence of any meaningful support for the proposition that appellant or other members of an armed group like al Qaeda qualify as lawful or privileged belligerents under the law of armed conflict, and upon consideration of the charged conduct and the entire record, we also conclude, beyond any reasonable doubt, that appellant was an AUEC as defined in the 2006 M.C.A.

(2) Conduct in the Context of and Associated with an Armed Conflict - Common Element 2

The 2006 M.C.A., as implemented in the 2007 M.M.C., requires a nexus between the charged conduct and an armed conflict to be punishable. This nexus performs an important narrowing function in determining which charged acts of terrorism constitute conduct punishable by such a law of war military commission, while effectively excluding from their jurisdiction isolated and sporadic acts of violence not within the context of an armed conflict. The 2007 M.M.C. includes this nexus as an element, requiring proof beyond a reasonable doubt that the offense occurred in the context of an armed conflict. 63

This element, sometimes referred to as the "contextual element" or "chapeaux," 64 is central to determining whether conduct is punishable by a law

---


63 See also Charge sheet. The 2006 M.C.A. limits jurisdiction over persons subject to trial by military commission to AUECs "engaged in hostilities or who has purposefully and materially supported hostilities." § 948a(1)(i) and § 948b(a)(emphasis added). See nn. 23, 24, 53. See also M.M.C., Part IV ¶ 6(a)(25). The scope of the conspiracy and solicitation offenses are limited to certain object offenses listed in the 2006 M.C.A. The seven objects of the conspiracy, in the Specification of Charge I, and solicitation, in the Specification of Charge II, are defined as an offense punishable by military commission in the 2006 M.C.A. §§ 950v(b)(1), 950v(b)(2), 950v(b)(3), 950v(b)(15), 950v(b)(16), 950v(b)(24), and 950v(b)(25). See infra pp. 89, 98.

of war tribunal. Consistent with treaty law, custom, and practice, the
determination whether the hostilities in issue satisfy this element is objective in
nature and generally relate to the intensity and duration of those hostilities.⁶⁶

In this case, each specification states that all conduct occurred in “various
locations in Afghanistan, Pakistan, and elsewhere.” Appellant has not
challenged the existence of an armed conflict between the United States and al
Qaeda, either at trial or on appeal. In Hamdan, the Supreme Court found an
armed conflict to exist with al Qaeda, one governed by applicable conventional
and customary laws of war. Hamdan 548 U.S. at 628-31. See supra n. 48. There
is no dispute that hostilities rising to the level of armed conflict existed in
Afghanistan, Pakistan and elsewhere including the United States no later than
September 11, 2001. After consideration of the record in this case, we conclude
that hostilities rising to the level of armed conflict existed on or before
February 1999 – the beginning of the charged timeframe. Again, the military
commission’s application of this contextual element proves illustrative. The
military commission judge instructed the members that:

With respect to each of the offenses listed as objects in the Specification
of charges, the government must prove beyond a reasonable doubt that the

---

⁶⁶ Leila Nadya Sadat and S. Richard Carden, The New International Criminal Court: An
are generally found in the chapeaux of the articles defining the crimes. The question arises in
war crimes, for example, as to whether an offense was committed in an armed conflict, and
whether that armed conflict was international or non-international in character.”)(emphasis
added).

⁶⁶ See APII, supra n. 39, art. 1.1 (“This Protocol which develops and supplements Article
3 common to the Geneva Conventions of 12 August 1949 without modifying its existing
conditions of application, shall apply to all armed conflicts which are not covered by Article
1 of [API] and which take place in the territory of a High Contracting Party between its
armed forces and dissident armed forces or other organized armed groups which, under
responsible command, exercise such control over a part of its territory as to enable them to
carry out sustained and concerted military operations and to implement this Protocol.”)
(emphasis added) and art 1.2. (“This Protocol shall not apply to situations of internal
disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts
of a similar nature, as not being armed conflicts.”); see also Rome Statute of the ICC, supra
nn. 51, 118, art. 8(2)(f) (“Paragraph 2(e) [lists 12 serious violations of the laws and customs]
“within the established framework of international law” that are applicable “to armed
conflicts not of an international character and ... not applicable to situations of internal
disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts
of a similar nature. It applies to armed conflicts that take place in the territory of a State
when there is protracted armed conflict between governmental authorities and organized
armed groups or between such groups.”).
offense took place in the context of and was associated with armed conflict. In determining whether an armed conflict existed between the United States and al Qaeda and when it began, you should consider the length, duration, and intensity of the hostilities between the parties; whether there was protracted armed violence between the governmental authorities and organized armed groups; whether and when the United States decided to employ the combat capabilities of its armed forces to meet the al Qaeda threat; the number of persons killed or wounded on each side; the amount of property damage on each side; statements of the leaders of either side indicating their perceptions regarding the existence of an armed conflict including the presence or absence of a declaration to that effect; and any other facts and circumstances you consider relevant to the existence of armed conflict. . . [Y]ou should consider whether [the charged offense] occurred during the period of an armed conflict as defined above; was intended or performed while the accused acted on behalf of or under the authority of a party to the armed conflict; and whether it constituted or was closely and substantially related to hostilities occurring during the armed conflict . . . . Conduct of the accused that occurs at a distance from the area of conflict or prior to the start of the conflict can still be in the context of and associated with armed conflict as long as it was closely and substantially related to the hostilities that comprised conflict.

Tr. 844-45.

In conclusion, the requirement that the charged conduct occur “in the context of and associated with an armed conflict,” as defined in the M.M.C. and by the military commission judge at trial are consistent with the law of armed conflict and the 2006 M.C.A. This element is fundamental to the military commission’s proper exercise of jurisdiction over any charged offense. Moreover, after weighing all the evidence in the record and recognizing that we did not see or hear the witnesses, we are also convinced, beyond a reasonable doubt, that the United States was engaged in an armed conflict with al Qaeda during the charged timeframe in “various locations in Afghanistan, Pakistan, and elsewhere.”

VIII. PROVIDING MATERIAL SUPPORT FOR TERRORISM, EX POST FACTO, AND INSTRUCTIONAL ERROR

We begin our analysis by combining appellant’s three challenges to the charge of providing material support for terrorism: (1) that providing material support for terrorism is not an offense punishable by military commission; (2) that this offense violated the Ex Post Facto Clause of the U.S. Constitution; and (3) that the military commission judge erroneously defined providing material support for terrorism at trial. Brief for Appellant 23-30; Reply Brief for Appellant 11-14.
A. Providing Material Support for Terrorism – an Offense under the Law of Armed Conflict

Appellant alleges that “Providing Material Support for Terrorism” is a “novel domestic crime” neither recognized nor charged as a war crime before passage of the 2006 M.C.A. Brief for Appellant 24; Reply Brief for Appellant 11-13.\(^{67}\) He also argues that, as an inchoate offense, providing material support for terrorism was not punishable by military commission. Brief for Appellant at 23-29; Reply Brief for Appellant 11-13. Finally, he avers that even assuming the offense was punishable by military commission the military commission judge erroneously defined that offense. Brief for Appellant at 29-30; Reply Brief for Appellant 13-14.

In *Hamdan*, we recently concluded that a military commission properly exercised jurisdiction under the 2006 M.C.A. over the charged conduct in five specifications of “providing material support for terrorism” when committed by an AUEC in the context of an armed conflict with the requisite knowledge and intent. *See Hamdan*, 2011 WL 2923945 at *18 (citations omitted). The conduct detailed in those five specifications was charged under two distinct formulations of the offense of providing material support for terrorism.

We disagree with appellant’s primary assertion that the charged conduct was not punishable by military commission when he committed the offenses. *See Hamdan*, 2011 WL 2923945 at *43-*44, *50 (citations omitted). The charged conduct, including appellant’s pledge of fealty to bin Laden, membership in al Qaeda, and intentional provision of material support or resources to al Qaeda, an international terrorist organization, then engaged in armed conflict with the United States, with knowledge that al Qaeda had engaged in or engages in terrorism, was punishable by military commission when committed.

1. The Charge

Appellant was charged in the Specification of Charge III with and convicted of:

[as an AUEC and in the context of an armed conflict from in or about February 1999 through in or about December 2001] at various locations in Afghanistan and elsewhere, intentionally provid[ing] material support and resources to al Qaeda, an international terrorist organization then engaged in hostilities against the United States, including violent attacks on the United States’ embassies [in] Nairobi, Kenya and Dar es Salaam, Tanzania [on] August 7, 1998; on the U.S.S. COLE [near] Aden, Yemen [on] October 12, 2000, and; at various locations in the United States [on]

\(^{67}\) *See also* Elsea, CRS Report No. R40752, *supra* n. 16, at 10 (“Similarly, defining as a war crime the ‘material support for terrorism’ does not appear to be supported by historical precedent.”).
September 11, 2001, knowing that al Qaeda engaged in or engages in terrorism, by:

a. traveling to Afghanistan with the purpose and intent of joining al Qaeda;

b. meeting with Saif al 'Adl, the head of the al Qaeda Security Committee, as a step toward joining the al Qaeda organization;

c. undergoing military-type training at an al Qaeda sponsored training camp then located in Afghanistan near Mes Aynak;

d. pledging fealty, or “bayat” to the leader of al Qaeda, Usama bin Laden, joining al Qaeda, and providing personal services in support of al Qaeda;

e. preparing and assisting in the preparation of various propaganda products, including the video “The Destruction of the American Destroyer U.S.S. COLE,” to solicit material support for al Qaeda, to recruit and indoctrinate personnel to the organization and objectives of al Qaeda, and to solicit, incite, and advise persons to commit terrorism;

f. acting as personal secretary and media secretary of Usama bin Laden in support of al Qaeda;

g. arranging for Muhammed Atta, also known as Abu Abdul Rahman al Masri, and Ziad al Jarrah, also known as Abu al Qa’qa al Lubnani, to pledge fealty or “bayat” to Usama bin Laden;

h. preparing the propaganda declarations styled as martyr wills of Muhammed Atta and Ziad al Jarrah in preparation for the acts of terrorism perpetrated by the said Muhammed Atta, Ziad al Jarrah and others at various locations in the United States on September 11, 2001;

i. at the direction of Usama bin Laden, researching the economic effect of the September 11, 2001 attacks on the United States, and providing the result of that research to Usama bin Laden; [and]

j. operating and maintaining data processing equipment and media communications equipment for the benefit of Usama bin Laden and other members of the al Qaeda leadership.

The charged conduct shares some commonality with Hamdan’s conviction for that same offense, as both Hamdan and al Bahlul received military-type training at an al Qaeda-sponsored training camp, both pledged fealty to bin Laden, both were al Qaeda members, and both provided personal services to bin Laden in support of al Qaeda’s goals and objectives. However, unlike Hamdan’s
more traditional soldier-like support (e.g. armed physical security and transportation of persons and weapons), appellant provided staffing and strategic support, and was acquitted of providing physical security.

2. The 2006 M.C.A. and 2007 M.M.C.

The 2006 M.C.A.’s definition of “Providing Material Support for Terrorism” includes two principal formulations of conduct comprising that offense. The first, not alleged here, includes “provid[ing] material support . . . for, or in carrying out an act of terrorism.” 2006 M.C.A. § 950v(b)(25)(A). While the second, charged here, is that the accused “intentionally provide[d] material support or resources to an international organization engaged in hostilities against the United States. . . .” *Id.* These two formulations are legally distinct. Accordingly, our analysis and holding pertain only to the second.

The 2007 M.M.C. in Part IV, ¶ 6(25)bB, lists the particular elements for providing material support for an international terrorist organization as follows:

B. (1) The accused provided material support or resources to an international terrorist organization engaged in hostilities against the United States;
   (2) The accused intended to provide such material support or resources to such an international terrorist organization;
   (3) The accused knew that such organization has engaged or engages in terrorism; and
   (4) The conduct took place in the context of and was associated with an armed conflict.

a. Material Support or Resources

The statute defines “material support or resources” as “any, property, tangible or intangible, or [any] service[].”*69* This definition includes a

---

*68* 2006 M.C.A. § 950v(b)(25)(A) (“Offense.—Any person subject to this chapter who [1] provides material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, an act of terrorism (as set forth in paragraph (24)), or [2] who intentionally provides material support or resources to an international terrorist organization engaged in hostilities against the United States, knowing that such organization has engaged or engages in terrorism (as so set forth), shall be punished as a military commission under this chapter may direct.”)(emphasis added)). *See also* 2007 M.M.C., Part IV, ¶ 6(25)b; *Hamdan*, 2011 WL 2923945 at *4-*5 (Hamdan was convicted of both types of providing material support for terrorism).

*69* *See* 2006 M.C.A. § 950v(b)(25)(B) (“[T]he term ‘material support or resources’ has the meaning given that term in section 2339A(b) of title 18.”). Title 18 U.S.C. § 2339A(b) reads:

(1) the term “material support or resources” means any property, tangible any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice
nonexclusive list of property and services constituting material support or resources including "expert advice or assistance, . . . communications equipment, . . . [and] personnel (1 or more individuals who may be or include oneself)[.]"  

By defining "material support or resources" as "any, property . . . or [any] service" Congress cast a wide net with respect to the scope of support and resources subject of the statute. The Supreme Court acknowledged the broad "scope" of this definition, in ruling on a recent challenge to the domestic law source of this definition. "Of course, the scope of the material-support statute may not be clear in every application." Holder v. Humanitarian Law Project, 561 U.S. ___, 130 S. Ct. 2705, 2720, 177 L. Ed. 2d 355 (2010). 

In this case, the Specification of Charge III states appellant provided both material support and resources. The primary resource charged was that he provided himself to al Qaeda as a member; consistent with the statute's explicit recognition of "personnel [including] oneself" as material support or resources. See 2006 M.C.A. § 950v(b)25(A) (quoted supra at nn. 68-69,). The specification states he traveled to Afghanistan to join al Qaeda, met with an al Qaeda leader, underwent military-type training at an al Qaeda sponsored camp, met with and pledged personal loyalty to bin Laden, and then joined al Qaeda. The Specification of Charge III ¶¶ a – d. 

Appellant was also charged with providing services in direct support of bin Laden and al Qaeda including; preparation of propaganda products intended for al Qaeda recruiting and indoctrination training, and inciting persons to commit terrorism; acting as personal and media secretary for bin Laden, facilitating the pledges of loyalty to bin Laden and preparing the propaganda declarations styled as Martyr Wills for two suspected September 11, 2001 hijackers/pilots, researching the economic effect of those attacks on the United States and providing the results to bin Laden, and operating and maintaining data processing equipment and media communications equipment for the benefit of bin Laden and other al Qaeda leaders. The Specification of Charge III ¶¶ e-j. 

or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials; (2) the term "training" means instruction or teaching designed to impart a specific skill, as opposed to general knowledge; and (3) the term "expert advice or assistance" means advice or assistance derived from scientific, technical or other specialized knowledge.). We interpret the language "any property, tangible or intangible, or service," to mean "any, property . . . or [any] service."

70 We interpret the word "including" to mean "includ[ing] but not limited to[.]" See 10 U.S.C. § 101(f)(4) ("Rules of Construction" "In this title . . . ‘includes’ means ‘includes but is not limited to’"). See also 2008 MCM, R.C.M. 103 Discussion.
Although the services he provided are not explicitly identified in the statute, the statutorily enumerated examples are a non-exhaustive list. The charged services fall within the scope of the statutorily defined services to include expert advice or assistance.

After review of the record, including the Specification of Charge III, and pleadings of the parties, we conclude that appellant's provision of himself as a member of al Qaeda and his provision to al Qaeda of various services constitute "material support or resources," as those terms are defined in the 2006 M.C.A.

b. Terrorism - defined

The offense of "terrorism" warrants particularized discussion as it is invoked in each charged offense. The 2006 M.C.A. § 950v(b)(24) prohibits AUECs from committing terrorism stating:

TERRORISM.—Any person subject to this chapter who intentionally kills or inflicts great bodily harm on one or more protected persons, or intentionally engages in an act that evinces a wanton disregard for human life, in a manner calculated to influence or affect the conduct of government or civilian population by intimidation or coercion, or to retaliate against government conduct, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

This definition of "terrorism," is incorporated into "providing material support for terrorism," see n. 68 (quoting 2006 M.C.A. 950v(b)(25)(A)), and may be appropriately characterized as the underlying offense. In addition, the specifications of the conspiracy and solicitation charges cite "terrorism" as an object offense. Accordingly, we will discuss "terrorism" as that offense is defined in the 2006 M.C.A. and international law.

The 2006 M.C.A. definition is more comprehensive than Common Article 3 of the Geneva Conventions, API, and APII. All prohibit the "intentional targeting and killing of protected persons" and "acts or threats of violence the primary purpose of which is to spread terror among the civilian population." See supra n. 39. In addition, the 2006 M.C.A. requires the Government prove that "[t]he accused did so in a manner calculated to influence or affect the conduct of government or civilian population by intimidation or coercion, or to retaliate against government conduct." 2007 M.M.C. Part IV, ¶ 6(24)b(2). The 2006 M.C.A.'s inclusion of an additional element actually narrows the conduct subject to individual criminal liability, and places an additional burden of proof on the Government.
The 2006 M.C.A. definition is also consistent with the most comprehensive definition of “terrorism” by international treaty extant on September 11, 2001. Specifically, the 1999 Financing Terrorism Convention included in its prohibition of conduct meeting the definition of terrorism:

Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out: (a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.


The similarity in these definitions does not suggest that a universally accepted definition of terrorism existed at the time of appellant’s charged conduct, or that such a definition currently exists in international law. A more accurate description of the treaty law addressing international terrorism would be ad hoc. Long-standing efforts to define “terrorism” have been the subject of persistent political dispute, primarily associated with national liberation movements, concerns inapplicable to al Qaeda’s attacks on the United States. See Alex Schmid, Terrorism on Trial: Terrorism—The Definitional Problem, 36 Case W. Res. J. Intl. L. 375 (2004).

At least 12 antiterrorism treaties or conventions predate appellant’s offenses. Describing terrorism as a crime of international significance, each of

---


the treaties oblige the parties to criminalize various facets of terrorism in their domestic criminal codes and to cooperate in the prevention and punishment of acts of terrorism. The Organization of American States Convention to Prevent and Punish the Acts of Terrorism Taking the Form of Crimes Against Persons and Related Extortion that are of International Significance, 27 U.S.T. 3949; T.I.A.S. 8413 (Feb. 2, 1971), ratified by the United States Oct. 8, 1976, Article 1, for example, provides:

[U]ndertake to cooperate among themselves by taking all the measures that they may consider effective, under their own laws, and especially those established in this convention, to prevent and punish acts of terrorism, especially kidnapping, murder, and other assaults against the life or physical integrity of those persons to whom the state has the duty according to international law to give special protection[.]

These conventions occurred in the context of numerous debates in the United Nations about the causes of international terrorism and ways to suppress and eliminate terrorism. A 1994 General Assembly Resolution on measures to eliminate international terrorism declared that:

1. The States Members of the United Nations solemnly reaffirm their unequivocal condemnation of all acts, methods and practices of terrorism, as criminal and unjustifiable, wherever and by whomever committed . . . ;

2. Acts, methods and practices of terrorism constitute a grave violation of the purposes and principles of the United Nations, which may pose a threat to international peace and security, jeopardize friendly relations among States, hinder international cooperation and aim at the destruction of human rights, fundamental freedoms and the democratic bases of society;

3. Criminal acts intended or calculated to provoke a state of terror in the
general public, a group of persons or particular persons for political
purposes are in any circumstance unjustifiable, whatever the
considerations of a political, philosophical, ideological, racial, ethnic,
religious or any other nature that may be invoked to justify them.[73]

In 1998, the Security Council adopted a resolution in response to the
attacks on the United States' embassies in Kenya and Tanzania, which are
named in the specification of the charge, by “[s]trongly condemn[ing] the
terrorist bomb attacks in Nairobi, Kenya and Dar-es-Salaam, Tanzania on 7
August 1998 which claimed hundreds of innocent lives, injured thousands of
S/RES/1189 (Aug. 13, 1998) at ¶ 1. In the same year, the Security Council
expressed its concern about “the continuing use of Afghan territory, especially
areas controlled by the Taliban, for the sheltering and training of terrorists and
the planning of terrorist acts, and reiterating that the suppression of
international terrorism is essential for the maintenance of international peace
and security,” and demanded “that the Taliban stop providing sanctuary and
training for international terrorists and their organizations.” S.C. Res. 1214,
U.N. Doc. S/RES/1214 (Dec. 8, 1998) at preamble and ¶ 13 (emphasis in
original).

The Organization of the Islamic Conference (OIC) was established on
September 25, 1969, and currently has 57 member countries with a total
population of 1.5 billion people. See OIC webpage on UN website,
Terrorism defines “Terrorism” as:

any act of violence or threat thereof notwithstanding its motives or
intentions perpetrated to carry out an individual or collective criminal
plan with the aim of terrorizing people or threatening to harm them or
imperiling their lives, honor, freedoms, security or rights or exposing the
environment or any facility or public or private property to hazards or
occupying or seizing them, or endangering a national resource, or
international facilities, or threatening the stability, territorial integrity,
political unity or sovereignty of independent States. [74]

---

[73] Declaration on Measures to Eliminate International Terrorism of 1994 (Elimination
Elimination Declaration was endorsed annually in subsequent UN resolutions.” Reuven
Young, Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International
Law and Its Influence on Definitions in Domestic Legislation, 29 B.C. Int'l Comp. L. Rev.

[74] OIC Convention on Combating International Terrorism ( Ouagadougou, Burkina Faso,
July 1, 1999) at pt. I, art. 1.2, http://www.oicun.org/7/38/. See also The League of Arab
States, Arab Convention for the Suppression of Terrorism, (Cairo, Apr. 22, 1998), pt. 1, art.
1.2 (using the same definition for terrorism); Hamdan, 2011 WL 2923945 at *21 and n. 65
There is ample evidence that an “intent” or “manner calculated to influence or affect the conduct of government . . . by intimidation or coercion,” supra p. 52, now constitutes “international custom, as evidence of a general practice accepted as law” or at minimum “the general principles of law recognized by civilized nations.” Statute of the International Court of Justice art. 38(1). This conclusion is based upon the implicit acceptance of the 1999 Financing Terrorism Convention’s definition of “terrorism” as it was signed by at least 39 nations before September 11, 2001, entered into force in April 10, 2002, and now has 132 signatories and 174 parties. See Hamdan, 2011 WL 2923945 at *20 n. 59 (listing number of signatories and parties). In addition, this requirement has routinely appeared in draft definitions emanating from the United Nations since the original working group report in November 2001, and in varying forms in domestic counter-terrorism laws.\textsuperscript{75} From 2001 to 2006, the United States sent five reports to the UN Security Council Committee on Counter-Terrorism describing efforts to suppress terrorism. See SCOR S/2006/397 (June 16, 2006); SCOR S/2006/69 (Feb. 3, 2006); SCOR S/2004/296


The UN General Assembly has issued numerous Resolutions addressing measures to prevent international terrorism. UN Action to Counter Terrorism Webpage (listing more than 60 UN General Assembly Resolutions to suppress or eliminate terrorism, http://www.un.org/terrorism/resolutions.shtml See, e.g., A/RES/65/34 (Jan. 10, 2011) at p. 3, ¶ 1 ("[s]trongly condemning all acts, methods and practices of terrorism in all its forms and manifestations as criminal and unjustifiable, wherever and by whomsoever committed;” and listing eight prior counter-terrorism resolutions from 2002 to 2009).
1. Non-U.S. Domestic Providing Material Support for Terrorism-Type Laws

The domestic laws of many nations prohibit conduct that is similar to providing material support for terrorism. Under Afghan law, for example, membership in a terrorist organization, recruiting another to commit a terrorist act, or helping in any form or way in order to complete the commission of a terrorist act is a crime. Law on Combat Against Terrorist Offenses, Art. 19 (July 2008). Article 3(1) of this law defines "Terrorist Offenses" and Article 3(2) defines "Terrorist and Terrorist Organizations" as a "real or legal person which has committed one of the offences mentioned in this Law or designated as a terrorist or terrorist organization by Resolution of the Security Council of the United Nations, provided that the Resolution is certified by the National Assembly."

Brazilian law punishes whoever:

destroys, sacks, extorts, robs, kidnaps, imprisons, burns, plunders, causes to explode, makes a personal attack, or performs acts of terrorism, due to political nonconformity or to obtain funds to be used to support organizations of a political or subversive nature . . . [whoever works to] establish, join, or maintain an illegal military organization of any type or nature, armed or not, with or without uniforms, whose purpose is to engage in combat.77

Egypt promulgated Law No. 97 in 1992, and amended it to address terrorist acts and terrorism "committed anywhere in the world." SCOR Report S/2001/1237 at 3 (Dec. 21, 2001) (citing Law No. 97 of 1992). "'[T]errorism’ means any use of force or violence or any threat or intimidation to which the perpetrator resorts in order to carry out an individual or collective criminal plan aimed at disturbing the peace or jeopardizing the safety and security of society and which” harms or creates fear or “imperil[s person’s] lives, freedoms or security; harm[s] the environment; damage[s] or take[s] possession of communications; prevent[s] or impede[s] the public authorities in the


performance of their work; or thwart[s] the application of the Constitution or of laws or regulations.” *Id.* at 4. The legislator incorporated this definition into criminalizing texts. *Id.*

The “cornerstone” of French counter-terrorism law is the Act of Sept. 9, 1986. SCOR Report S/2001/1274 at 3 (Dec. 27, 2001). “Terrorist acts are generally defined by combining the existence of an offence under ordinary criminal law which appears on a restrictive list with an ‘individual or collective undertaking, the aim or which is to cause a serious disturbance to public order by means of intimidation or terror.” *Id.* Some offenses such as “membership of terrorist groups” have separate legal definitions. *Id.*

The Terrorist and Disruptive Activities (Prevention) Act (1987) (1987 TADA) of India prohibits terrorists acts stating, “Whoever with the intent to overawe the Government . . . or to strike terror . . . in any section of the people . . . or to adversely affect the harmony amongst different sections of the people does any act or thing.” 1987 TADA, Ch I, Pt. II, ¶ 3(1). It broadly describes the prohibited means and objectives for commission of a terrorist act:

by using . . . weapons . . . or by other substances . . . of a hazardous nature . . . to cause, or as is likely to cause, death of, or injuries to, any person or persons. . . . [causing the] loss of, or damage to, or destruction of, property or disruption of any supplies or services essential to the life of the community, [and threatening] to kill or injure such person in order to compel the Government or any other person to do [or refrain] from doing any act.

*Id.* See also *Hamdan*, 2011 WL 2923945 at *26 (citations omitted) (describing in more detail the development of counter-terrorism law in India).

Indonesian law punishes “[a]ny person who with deliberate intent sets fire, causes explosion or causes a flood.” SCOR Report S/2001/1245 at 7 (Dec. 26, 2001) (citing Penal Code of Indonesia, Book II on Crimes, Ch. VII on Crimes whereby the General Security of Persons or Property is Endangered, art. 187). Whoever “produces, receives, tries to procure, . . . conceals, transports or imports into Indonesia . . . objects . . . of which he knows or reasonably must suspect that they are intended . . . to cause an explosion, whereby danger of life or general danger to property is feared” commits an offense. *Id.* The Government Regulation in Lieu of Legislation of the Republic of Indonesia No. 1/2002 on Combating Criminal Acts of Terrorism penalizes the intentional use of violence or the “uses violence or the threat of violence to create a widespread atmosphere of terror or fear in the general population or to create mass casualties, by forcibly taking the freedom, life or property of others or causes damage or destruction to . . . the environment or public facilities or international facilities.” *Id.* at Ch. III, §§ 6, 7 (Oct. 18, 2002).
Italy implemented measures in the 1960s and 1970s to combat domestic terrorism, and adopted additional measures to combat international terrorism after September 11, 2001. Elies van Sliedregt, *European Approaches to Fighting Terrorism*, 20 Duke J. Comp. & Intl. L. 413, 420 (2010); SCOR Report S/2002/8 at 4-6 (Jan. 2, 2002). The Cossiga Law, enacted on February 6, 1980, punished "[mere participation in]...an "association with the aim of terrorism and of subversion of the democratic order’ and ‘attack for subversive or terrorist purposes’" without the necessity of actual participation in a violent act.\(^{78}\)

Japan’s counter-terrorism strategy utilizes the Subversive Activities Prevention Act, which prohibits a variety of terrorism-related activities, including causing, preparing, plotting, and aiding in internal disturbance; as well as actions to induce, aid, plot, preparation or attempt to induce foreign incursion.\(^{79}\)

Pakistan adopted the Anti-Terrorism Act of 1997 (1997 ATA) to prevent terrorist acts. SCOR Report S/2001/1310 at 6 (Jan. 10, 2002). “In August 2001, the [1997 ATA] was further amended to enlarge its scope. Under the amended Act, terrorism is a punishable offence and abetting terrorism, including membership of terrorist groups and recruitment and support for such groups, is an offence.” *Id.* “Sections 11(A) to 11(X) [of the 1997 ATA as amended] prohibit organizations involved in terrorist activities and bars membership and support to such organizations.” *Id.* at 8. *See also Hamdan*, 2011 WL 2923945 at *26-*27 (citations omitted) (describing in more detail Pakistan’s counter-terrorism laws). The ATA (Second Amendment) Ordnance XIII 1999, § 6 (Gazette of Pakistan, Extraordinary, Pt. I, Aug. 27, 1999), which provides:

A person...commit[s] a terrorist act if he, (a) in order to, or if the effect of his actions will be to, strike terror or create a sense of fear and insecurity in the people, or any section of the people does any act or thing by using bombs, dynamite or other explosive or inflammable substances, or such fire-arms or other lethal weapons...in such a manner as to cause or be likely to cause, the death of or injury to any person or persons or damage to or destruction of, property on a large scale,...or threatens with the use of force public servants in order to prevent them from
