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 David 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."[1]

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.[2] 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

---

[1] Transcript available at http://www.pbs.org/newshour/bb/terrorism/jan-jun11/panetta_05-03.html (last visited Sept. 8, 2011).

[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.[3] 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."[4] 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.

Interview by Greg Bruno with James A. Lewis, Director, Techn. & Pub. Policy Program, Ctr. for Strategic & Int'l Studies, (Dec. 28, 2009), *available at* http://www.cfr.org/publication/21052/prioritizing_us_cybersecurity.html?breadcrumb=%2Fbios%2F13554%2Fgreg_bruno.

[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, employment 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.[5] Advocates of military transparency want to ensure the reputation of America's men and women in uniform remains untarnished by association with the shadowy world of espionage.[6] 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."[7] 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.

[8] Jennifer D. Kibbe, *The Rise of the Shadow Warriors*, 83 FOREIGN AFFAIRS 102, 113 (March/April 2004), *available at* http://users.polisci.wisc.edu/kinsella/Rise%20of%20the%20shadow%20warriors.pdf.

[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.

[12] The Pentagon's efforts to create a human intelligence capability separate from and seemingly parallel to the CIA's human intelligence capabilities is seen as encroaching "on the CIA's realm." ALFRED CUMMING, CONGRESSIONAL RESEARCH SERVICE, COVERT ACTION: LEGISLATIVE BACKGROUND AND POSSIBLE POLICY QUESTIONS 3 (2009). *See also* Eric Schmitt and Thom Shanker, *Threats and Responses: A CIA Rival; Pentagon Sets Up Intelligence Unit*, N.Y. TIMES, Oct. 24, 2002, at A1, *available at* http://www.nytimes.com/2002/10/24/world/threats-and-responses-a-cia-rival-pentagon-sets-up-intelligence-unit.html.

[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."[15] 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.

---

spy satellites and overseas listening posts. Mark Mazzetti, *Nominee Promises Action as U.S. Intelligence Chief*, N.Y. TIMES Jul. 21, 2010, at A16, *available at* http://www.nytimes.com/2010/07/21/us/politics/21intel.html.

[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.[16] 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.[17]

Professor McNeal's hypothetical evidences a misunderstanding or mischaracterization of the law and conduct of military operations.[18] 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 authorities. 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).[19] 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.

[20] James E. Baker, *National Security Process: Process, Decision, and the Role of the Lawyer*, *in* NATIONAL SECURITY LAW 911, 913 (John Norton Moore & Robert F. Turner, eds., 2d ed. 2005).

[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[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."[23] As chief executive, the President may "manage the business of intelligence in such a manner as prudence may dictate."[24] This includes the authority to secretly collect intelligence for reasons of national security.[25] As commander in chief, the President may employ the military to protect the national interests of the United States as he deems necessary.[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.[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

---

[22] U.S. CONST. art. II, § 1.
[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).
[24] THE FEDERALIST No. 64 (John Jay).
[25] *See, e.g.*, Chicago & S. Air Lines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948); Totten 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.").
[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).
[27] U.S. CONST. art. I, § 8, cls. 1 & 11–13.

anticipated.[28] The President must generally withdraw the military forces within sixty days unless Congress formally declares war or otherwise authorizes the combat deployment.[29] 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."[30]

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."[31] 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."[32]

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

---

[28] 50 U.S.C. §§ 1541–1548 (1973).

[29] Two key provisions in 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.

[31] Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 HARV. L. REV. 2047, 2051 (2005).

[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

---

[33] *See generally* JOHN YOO, CRISIS AND COMMAND: A HISTORY OF EXECUTIVE POWER FROM GEORGE WASHINGTON TO GEORGE W. BUSH (2009); JOHN YOO, THE POWERS OF WAR AND PEACE (2005); Phillip Bobbitt, *War Powers: An Essay on John Hart Ely's War and Responsibility: Constitutional Lessons of Vietnam and its Aftermath*, 92 MICH. L. REV. 1364, 1373 (1994); Henry P. Monaghan, *Presidential War-Making*, 50 B.U. L. REV. 19 (1970); Eugene V. Rostow, *Great Cases Make Bad Law: The War Powers Act*, 50 TEX. L. REV. 833 (1972); John Yoo, *The Continuation of Politics by Other Means: The Original Understanding of War Powers*, 84 CAL. L. REV. 167 (1996).

[34] Harold H. Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair*, 97 YALE L.J. 1255, 1282 (1998). *See also* JOHN HART ELY, WAR AND RESPONSIBILITY: CONSTITUTIONAL LESSONS OF VIETNAM AND ITS AFTERMATH 3–5 (1993); LOUIS FISHER, PRESIDENTIAL WAR POWER 3–12 (1995); MICHAEL J. GLENNON, CONSTITUTIONAL DIPLOMACY 80–84 (1990); HAROLD H. KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN-CONTRA AFFAIR 74–77 (1990); Bruce Ackerman, *The Emergency Constitution*, 13 YALE L. JOURNAL 1029, 1046–56 (2004); Raoul Berger, *War-Making by the President*, 121 U. PA. L. REV. 29, 39–47 (1972).

[35] FISHER, *supra* note 34, at 11.

[36] Jack Goldsmith, *The Accountable Presidency*, THE NEW REPUBLIC (Feb. 1, 2010), http://www.tnr.com/article/books-and-arts/the-accountable-presidency.

rough way, the Framers' original design."[37] 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."[38]

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.[39] 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.[40]

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.[41] 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.[42]

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."[43] Title 10 gives the Secretary of Defense all "authority, direction and control" over DoD, including all subordinate agencies and commands.[44] Title 10 also created combatant commands, which include geographic commands (e.g., U.S.

---

[37] *Id.*
[38] *Id.*
[39] National Security Act of 1947, Pub. L. No. 235 (1947).
[40] 50 U.S.C. §§ 1–2420.
[41] 10 U.S.C. §§ 101–18505. Laws pertaining to the National Guard were transferred to Title 32.
[42] Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. 99–433 (1986).
[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).
[44] 10 U.S.C. § 113(b) (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.[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.[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.[47] The Secretary of Defense's control and direction of DoD human intelligence activities can be limited only by the President.[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."[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 . . . ."[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,[51] yet

---

[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.

[46] 10 U.S.C. § 167(j) (2006).

[47] 50 U.S.C. § 403–5 (2006).

[48] *Id.* at § 403–5(b)(5) (2006). *See also supra* note 10.

[49] 10 U.S.C. § 137 (2006); Pub. L. No. 107–314 (2002).

[50] E.O. 12,333, *supra* note 10, at ¶1.10.

[51] *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.[52] 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.[53]

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.

[52] *See* 50 U.S.C. §403-5(a) & (b) (2006).

[53] U.S. DEPARTMENT OF DEFENSE, JOINT PUBLICATION 3-0, DOCTRINE FOR JOINT OPERATIONS I-1 (Sep. 10, 2001).

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

[54] Jeffrey H. Smith, *Keynote Address: Symposium: State Intelligence Gathering and International Law*, 28 MICH. J. INT'L L. 543, 546–47 (2007). It should be noted that Smith was CIA General Counsel from May 1995 to September 1996. As such, his perspective very much reflects the national security mindset of the mid-1990s, which changed dramatically after the 9/11 attacks.

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.

[58] House Permanent Select Committee on Intelligence, Report to Accompany the Intelligence Authorization Act for Fiscal Year 2010, H.R. REP. NO. 111-2701 (Jun. 29, 2009) at 50.

[59] *Id.*

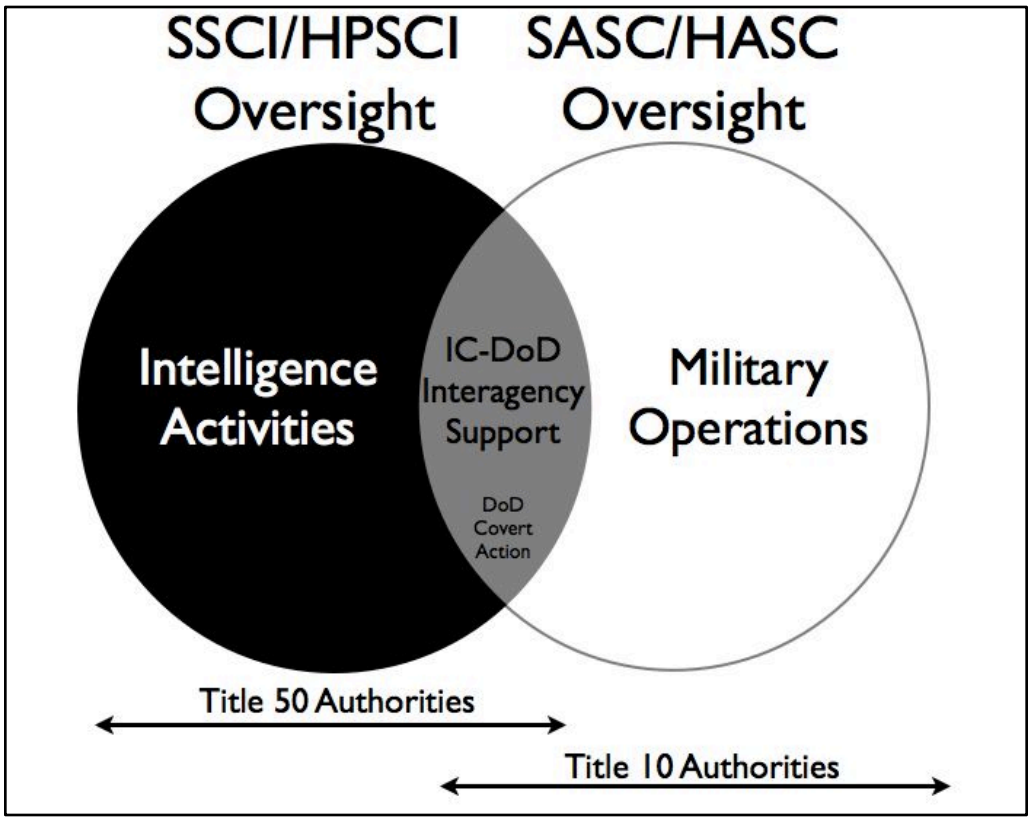

Figure 1: Congressional Oversight of Intelligence Activities and Military Operations

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.[60] 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.[61]

---

[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."[62] 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.[63] The Church Committee's subsequent investigation "did nothing less than revolutionize America's attitudes toward intelligence supervision."[64]

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].

[63] Loch K. Johnson, *The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability*, 23 INTELLIGENCE AND NAT'L SECURITY 198, 198–225 (2008).

[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."

[66] Intelligence Authorization Act for 1992, 105 Stat. 441, Pub. L. 102-88 (1991). The caveat regarding Constitutionality was deleted and the statute now provides: "The President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity." 50 U.S.C. § 413 (2010).

[67] The National Intelligence Program is defined as:

> [A]ll 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.

50 U.S.C. § 401(a) (2010). For a brief overview of intelligence nomenclature, see *supra* note 48.

[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."[69] 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.[70]

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.

[69] HOUSE RULES, Rule X, 11(b)(1)(B) (2009).

[70] *Id.* at Rule X, 11(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."

[72] FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 420 (Official Government Ed., 2004).

[73] 50 U.S.C. § 414 (2010).

[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.

Consolidated Security, Disaster, and Continuing Appropriations Act of 2009, § 8080, Pub. L. 110-329 (Sep. 30, 2008).

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.[75] 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.[76]

A former general counsel for the CIA suggested an erosion of distinctions between military operations and covert action in the context of cyberwarfare.[77] John Rizzo characterized the Title 10-Title 50 debate in

---

[75] *See generally* GARY BERNTSEN, JAWBREAKER (2005); HY S. ROTHSTEIN, AFGHANISTAN AND THE TROUBLED FUTURE OF UNCONVENTIONAL WARFARE 33 (2006); DOUG STANTON, HORSE SOLDIERS: THE EXTRAORDINARY STORY OF A BAND OF US SOLDIERS WHO RODE TO VICTORY IN AFGHANISTAN (2009).

[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.firedoglake.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."[78] 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.[79] 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."[80] Yet even Secretary of Defense Donald Rumsfeld reportedly questioned who was really in charge.[81] 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/natsecurity/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."[82] 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,[83] and 3) it supports "activities" against the government or occupying power.[84]

---

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.

[82] U.S. DEPARTMENT OF DEFENSE, JOINT PUBLICATION 3-05, DOCTRINE FOR JOINT SPECIAL OPERATIONS FORCES GL-13 (April 18, 2011).

[83] ARMY FIELD MANUAL FM 3-05.130, provides this distinction between regular and irregular forces:

> 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.
>
> 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."

[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.[85] These activities do not necessarily by themselves constitute unconventional warfare, but rather they typify tactics and techniques commonly employed in unconventional warfare.[86] 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.[87] 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."[88] Unconventional warfare "is fought by subterranean armies composed of volunteers, revolutionists, guerillas, spies, saboteurs, provocateurs, corrupters, [and] subverters," and it is waged

---

[85] ARMY FIELD MANUAL FM 3-05, *supra* note 83, at 130.

[86] "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. Kennedy Special Warfare Center and School located at Ft Bragg, North Carolina).

[87] 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.

[88] ROTHSTEIN, *supra* note 75, at 159.

through military, political, economic, and psychological means.[89] In peacetime, unconventional warfare "operates at a level below that of outright provocations and the instigators do not appear in the open."[90]

As we saw above, the U.S. military limits its definition of unconventional warfare to activities that take place within the context of insurgencies (conflicts in denied areas against the government or force in power). U.S. support to insurgencies "can be categorized as one of two types of campaign efforts: general war scenarios and limited war scenarios."[91] 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 Jedburg teams inserted by the Office of Strategic Services (OSS) into occupied France during World War II,[92] Afghanistan in 2001–2002,[93] and Iraq in 2003.[94]

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.[95] The United States conducted unconventional warfare in the context of limited war in North Vietnam in 1961–1964,[96] the

---

[92] OSS deployed 93 Jedburgh teams into German-occupied France. The three-man Jedburg teams parachuted into enemy territory and advised, coordinated and directed French resistance fighters as they conducted sabotage and guerilla attacks against German forces. C.I.A., THE OFFICE OF STRATEGIC SERVICES: AMERICA'S FIRST INTELLIGENCE AGENCY (2007), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/oss/art05.htm; MILTON J. SHAPIRO, BEHIND ENEMY LINES (1978).

[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. GRDOVIC, *supra* note 86, at 7.

[95] *See generally* MAX BOOT, THE SAVAGE WARS OF PEACE: SMALL WARS AND THE RISE OF AMERICAN POWER (2002); PETER HARCLERODE, FIGHTING DIRTY (2001); JOHN J. TIERNEY, JR., CHASING GHOSTS: UNCONVENTIONAL WARFARE IN AMERICAN HISTORY (2006).

[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 guerilla attacks. *See generally* RICHARD H. SHULTZ

Bay of Pigs in 1961, Nicaragua in 1980–1988,[97] and Afghanistan in 1980–1989.

Unconventional warfare is generally effectuated in seven phases: preparation, initial contact, infiltration, organization, buildup, employment, and transition.[98] Each phase may not always be required, and phases may be conducted simultaneously or out of sequence.[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.[100] SOF often augment pilot teams led by, and primarily constituted of, CIA personnel.[101]

JR., THE SECRET WAR AGAINST HANOI (1999); MARK H. WAGGONER, MILITARY ASSISTANCE COMMAND VIETNAM: COMMAND HISTORY (1970), esp. Annex B: Studies and Observations Group.

[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.

[98] ARMY FIELD MANUAL FM 3-05.130, *supra* note 83, at 4-4.

[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.*

[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.

[101] *Id.* at 5-2. 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

---

[102] The Center for Strategic and International Studies compiled a list of 68 "significant cyber incidents" between 2006 and 2011. JAMES ANDREW LEWIS, CYBER EVENTS SINCE 2006, CSIS (Jan. 25, 2001), *available at* http://dev.csis.org/publication/cyber-events-2006. *See also* RICHARD A. CLARKE AND ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010); Ellen Nakashima, *For Cyberwarriors, Murky Terrain; Pentagon's Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Policies*, WASH. POST, Mar. 19, 2010, at A1.

[103] MCAFEE, VIRTUAL CRIMINOLOGY REPORT 2009, VIRTUALLY HERE: THE AGE OF CYBERWARFARE 13 (2009).

[104] William J. Broad, John Markoff and David E. Sanger, *Israel: Test on Worm Called Crucial in Iran's Nuclear Delay*, N.Y. TIMES, Jan. 16, 2011, at A1.

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.[105] If true, Stuxnet heralded a new age of cyberwarfare able to destroy "targets with utmost determination in military style."[106]

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."[107] 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

---

[105] Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR, April 2011, at 152–59, 195–98.

[106] Broad et al., *supra* note 104.

[107] Robert F. Gates, Memorandum: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations, Department of Defense (Jun. 23, 2009).

operations.[108] 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."[109]

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."[110] 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."[111] 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."[112] Cyberspace is governed by the laws of physics and the logic of computer code.[113]

---

[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 60-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).

[111] Dan Kuel, *Cyberspace & Cyberpower: Defining the Problem*, *in* CYBERPOWER AND NATIONAL SECURITY 28 (Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz, eds., 2009).

[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.[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.[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

---

[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).

[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.[116] 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.[117]

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

---

[116] 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." CARL VON CLAUSEWITZ, ON WAR 87 (Michael Howard & Peter Paret, eds. & trans., Princeton Univ. Press 1976) (1832). *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."

[117] 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.

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.
[120] NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin, eds., 2009).

Box 1—Cyberattack versus Cyberexploitation

	Cyberattack, attack, computer network attack	Cyberexploitation, intelligence, exploitation, computer network exploitation
Approach and intent	Degrade, disrupt, deny, destroy attacked infrastructure and systems/networks	Achieve smallest intervention consistent with desired operations
Relevant domestic law	U.S. Code Title 10 authorities and restrictions	U.S. Code Title 50 authorities and restrictions
Operational agency	U.S. Strategic Command (Joint Functional Component Command for Network Warfare)	National Security Agency
Main advocate in the U.S. government to date	U.S. Air Force	Director of National Intelligence
Interactions with tactical military operations	Based on explicit inclusion in battle plans	Based on intelligence reporting
Characterization of personnel	Warfighters	Intelligence community

Source: NATIONAL RESEARCH COUNCIL.

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."[121] The closest Title 50 comes to defining intelligence activities is its stipulation that the term includes "covert action" and "financial intelligence activities."[122] 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.[123] 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."[124]

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."[125] 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.[126] Indeed, so many elements of DoD are also

---

[121] 50 U.S.C. § 413(a)(1) (2006).
[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."
[124] 50 U.S.C. § 401a(6) (2006).
[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.[127]

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.

responsibilities."[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.[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

---

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

[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)." CONFERENCE REPORT ON THE INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1991, H.R. REP. NO. 102-166 (Conf. Rep.) (July 25, 1991) at 21 [hereinafter Conference Report].

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."[130] 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] 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.[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."[132] Accordingly, covert action consists of three essential elements:

---

[131] President Bush's signing statement reads, in pertinent part:

> 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.

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 Aggrandizement 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 briefs 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).

[132] 50 U.S.C. § 413b(e) (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.[133] 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."[134]

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."[135] It is not clear that the Executive Branch shares Congress's interpretation, nor are these congressional interpretations legally binding.[136] 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 anticommunist 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. TREVERTON, *supra* note 10, at 210.

[133] Pub. L. No. 102-88, §§ 601-603, 105 Stat. 429, 441-445 (1991), *as amended* (codified at 50 U.S.C. § 413-414).

[134] H.R. REP. NO. 102-166, *supra* note 129, at 28.

[135] AUTHORIZING APPROPRIATIONS FOR FISCAL YEAR 1991 FOR THE INTELLIGENCE ACTIVITIES OF THE U.S. GOVERNMENT, THE INTELLIGENCE COMMUNITY STAFF, THE CIA RETIREMENT AND DISABILITY SYSTEM, AND FOR OTHER PURPOSES, S.R. REP NO. 102-85 (Sen. Rep.) (June 19, 1991) at 42. The Conference Report does reference the Senate Report's explanation of the traditional military activities exception to covert action. H.R. REP. NO. 102-166, *supra* note 129, at 30.

[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.[137] 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.[138] 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."[139] 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."[140]

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[141] 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.*

[139] 50 U.S.C. § 413b(e) (2006).

[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,[143] 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.[144]

---

[143] 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).

[144] 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":

> 1. activities where the primary purpose is to collect intelligence;
> 2. traditional counterintelligence activities;
> 3. traditional operational security programs and activities;
> 4. administrative activities (e.g., pay and employee support);
> 5. traditional diplomatic activities and their routine support;
> 6. traditional military activities and their routine support;
> 7. traditional law enforcement activities and their routine support; or
> 8. routine support to the overt activities of the U.S. government.

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.[145] 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

---

H.R. REP. NO. 102–166, *supra* note 129, at 28–30.

[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."[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.[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.[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

---

[146] Conference Report, *supra* note 129 (emphasis added).

[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.

[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.[149]

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."[150] 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.[151] 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."[152] This point is particularly illuminating as the

---

[149] 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)).

[150] 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.

[151] 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 directing authority approves a military course of action." *Id.* at GL-20.

[152] Conference Report, *supra* note 129, at 30.

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.[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."[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

---

[153] *Id.* The Conference Report then refers readers to the Senate Report, which states

> The Committee also recognizes that even in the absence of anticipated or ongoing hostilities involving U.S. military forces there could potentially be requirements to conduct activities abroad which are not acknowledged by the United States to support the planning and execution of a military operation should it become necessary. Whether or not other forms of support for the planning and execution of military operations could constitute 'covert actions' will depend, in most cases, upon whether they constitute 'routine support' to a military operation."

S. REP. NO. 102-85, *supra* note 135, at 47. The Senate Report contained more restrictive language than what was included in the final Conference Report. For example, the Senate report found acknowledgement (or the lack thereof) to be a deciding factor, while the Conference Report rightfully concluded that the exercise of command and control is decisive. *Compare* Conference report, *supra* note 135, *with* S. REP. NO. 102-85 (1991) (Conf. Rep.). *See also* Gross, *infra* note 169, at 8. This issue was revisited in 2003 when the SSCI attempted to assert that unacknowledged operations in countries where U.S. military forces do not have an acknowledged presence would fall within the definition of covert action. The unclassified portion of the intelligence authorization act that passed the Senate in November 2003 did not include this controversial assertion and instead reaffirmed "the functional definition of covert action." Kibbe, *supra* note 8, at 107.

[154] Conference Report, *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.[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.[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.

---

[155] *Id.*

[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

---

[157] OPE is no longer defined in unclassified U.S. military publications, however it is considered "Pentagon-speak for gathering information in trouble spots around the world to prepare for possible missions." Linda Robinson, Plan of Attack, *The Pentagon Has a New Strategy For Taking on Terrorists-and Taking Them Down*, U.S. NEWS AND WORLD REPORT (Aug. 1, 2005), http://www.usnews.com/usnews/news/articles/050801/1terror.htm.
[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 expend 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."[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.[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.[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

---

[161] HPSCI Report, *supra* note 158, at 11.

[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).

[163] H.R. REP. NO. 101-725, pt. I (1990) (Conf. Rep.). DoD defines clandestine operation as

> 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."[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."[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."[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."[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."[168]

---

[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 USD(I) was dual-hatted by DNI McConnell to serve concurrently as his Deputy Director for Defense. Yet, the USD(I) 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 USD(I) 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).

[165] Blair, *supra* note 164, at 117.

[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.

[167] *Id.*

[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.[169] 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.

[169] *See generally* RICHARD C. GROSS, DIFFERENT WORLDS: UNACKNOWLEDGED SPECIAL OPERATIONS AND COVERT ACTION (2009), *available at* http://handle.dtic.mil/100.2/ADA494716.

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.

* * *