US Cyber Operations: Intelligence Activities or Military Operations?
Andru E. Wall

andru.wall@gmail.com
US Cyber Operations: Intelligence Activities or Military Operations?
Andru E. Wall

ABSTRACT: Cyber operations require close integration of intelligence and operational capabilities. The Secretary of Defense has authorities under Title 10 and Title 50 and is best suited to lead US government cyber operations against external threats. Title 10 and Title 50 create mutually supporting rather than mutually exclusive authorities. Cyber operations conducted pursuant to an execute order are military operations and not intelligence activities. Attempts by congressional overseers to redefine military preparatory operations as intelligence activities are legally unsupportable.

I. Introduction
A. Cyberspace & Cyberspace Operations 2
B. Cyber Command & The Title 10-Title 50 Debate 5

II. Operational Authorities or Congressional Oversight?
A. Presidential Power 8
B. Statutory Authorities 10
C. Congressional Oversight 12

III. Intelligence Activities or Military Operations?
A. Moving From Information Collection to Preparing the Environment 17
B. Why Operational Preparation of the Environment is Not Covert Action 19

IV. Concluding Analysis
A. Intelligence Activities 24
B. Military Operations 25
I. Introduction

The future of warfare is here. Cyberwarfare. Not yet the outbreak of a “hot” cyber war between major powers, but minor skirmishes, a silent cyber arms race, and major intelligence gathering. According to Mike Jacobs, formerly of the US National Security Agency, 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.”1 These may be acts of cyber espionage rather than cyberwarfare, but at a minimum they are preparing cyberspace for warfare.

Israel conducted a cyber attack on Syrian air defense systems in September 2007. Before bombs fell on a suspected nuclear weapons facility, Israel attacked Syrian air defense systems in cyberspace with the 1s and 0s of computer code — controlling what Syria saw and ensuring Israeli aircraft entered and departed Syrian airspace undetected.2

Just a few months later, American military personnel reportedly attacked a website — an online forum designed to lure wannabe terrorists. The site was covertly monitored by Saudi and American intelligence agencies who gleaned intelligence on terrorist recruitment networks. Military officials, however, thought the site was more effective at recruitment than intelligence gathering. Believing the website was facilitating attacks on American servicemen in Iraq, the US military attacked the website and inadvertently took down servers in Saudi Arabia, Germany and Texas.3

The United States is its preparations for cyberwarfare, but myriad questions remain. The primary concerns reflected in questions posed by Congressmen to General Keith Alexander, the Commander of the newly-established US Cyber Command, related to legal authorities — specifically, where is the line between cyber intelligence activities and military operations? This paper answers this question by framing the analysis and revealing the false dichotomy between Title 10 an Title 50.

A. Cyberspace & Cyberspace Operations

Cyberspace is defined by the US 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


3 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 A01.
processors and controllers.” Others suggest a definition that emphasizes cyberspace as a global information environment unique in its “use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communications technologies.” Indeed, the distinctive use of electronics and electromagnetic spectrum distinguishes cyberspace from the domains of land, sea, air and space: it is “a physical environment … managed by rules set in software and communications protocols.” Cyberspace is governed by the laws of physics and the logic of computer code.

Cyberwarfare is defined simplistically by Wikipedia as the use of computers and the Internet to conduct warfare in cyberspace. The US military does not define cyberwarfare in its unclassified dictionary, rightfully avoiding the term “war” with its associated baggage and implications. The US military instead categorizes cyber operations as either defense, exploitation, or attack. This paper focuses on the last two, exploitation and attack, and attempts to define the operational authorities and identify the type of activities associated with each.

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

---

4 US DEPARTMENT OF DEFENSE, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 139 (Apr. 12, 2001 as amended through April 2010). 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).

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


7 Id. at 255.

8 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).

9 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. US DEPARTMENT OF DEFENSE, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 95 (Apr. 12, 2001 as amended through Apr. 2010).
include acts of computer network exploitation where computer code is left behind or altered (e.g., 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. 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.

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 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 simply attempting to exploit your network. The other party knows why he is inside your network, but you don’t. If you know your network is being attacked, a broad range of responses may be justified in self-defense; however, if your network is merely being exploited (an intelligence activity) your range of responses are arguably more limited. Thus, this distinction helps define the operational authority to carry out an operation, but does 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 battle damage assessment.” In the words of one expert on cyber attack, “those who prepare and conduct operational cyberwar will have to inject

---

10 Defining warfare is beyond the scope of this paper, but suffice to say it involves the forced imposition of political will. It is, in Carl Von Clausewitz’s immortal words, the “continuation of political intercourse, carried on by other means.” Carl Von Clausewitz, On War 87 (Michael Howard & Peter Paret, eds. & trans., Princeton University Press 1976)(1832). See also Myres S. McDougal and Florentino P. Feliciano, The International Law of War: Transnational Coercion and World Public Order 11 (1994)(originally published as Law and Minimum World Public Order in 1961), which defines coercion as “a high degree of constraint exercised by means of any or all of the various instruments instruments of policy.”

11 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.

12 Martin C. Libicki, Cyberdeterrence and Cyberwar 139 (RAND, 2009).
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.”

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 collection, analysis, and action in milliseconds.

This is precisely why US Secretary of Defense Robert Gates 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 a lot of questions about authorities and oversight. After all, congressional oversight retains an antiquated organizational structure and presumes a strict separation between intelligence activities and military operations; we will see that no such separation is required by law.

B. Cyber Command & The Title 10-Title 50 Debate


Accepting the recommendation of Secretary Gates, President Barack Obama nominated Lieutenant General Keith B. Alexander, the Director of the National Security Agency, to also serve as the Commander of US Cyber Command. During the confirmation process, the Senate Armed Services Committee questioned various aspects of General Alexander’s proposed dual responsibilities. 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 US Cyber Command, a military war-fighting command?

These questions addressed what is colloquially referred to as “Title 10-Title 50 issues”. The Committee asked General Alexander, for example, about congressional oversight of Cyber Command’s “integrated intelligence collection”, whether intelligence support provided to Homeland Security would be an intelligence activity, whether the Department of Defense conducts intelligence gathering of foreign networks, whether intelligence gathering of foreign

13 Id. at 156.

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 provide important insight into how the Secretary of
Defense carries out his statutory and delegated authorities to carry out intelligence activities and
military operations. General Alexander repeatedly explained that “while there will be, by design,
significant synergy between NSA and Cyber Command, each organization will have a separate
and distinct mission with its own identity, authorities, and oversight mechanisms.”

Cyberspace is inherently global, interconnected and malleable, yet American instruments of
statecraft are generally organized, funded and controlled by separate and distinct “stove-piped”
authorities. The departments of State, Defense, Justice and Homeland Security are each lead by
a Secretary who reports only to the President, as does the Director of National Intelligence. The
National Security Council attempts to coordinate US national security policy across the various
departments and agencies, but only the President possesses the legal authority to settle
interagency disputes.

Congressional oversight and funding control further complicates interagency coordination and
cooperation. Each entity within the US national security apparatus has its own congressional
committee or subcommittee that acts, in essence, as its congressional handler. A codependency
of sorts exists between the congressional committees and the Executive Branch agency or
department as the former controls the purse strings and the latter controls information on its
activities.

Intelligence activities are further stove-piped. Following the passage of the National Security
Act of 1947 and continuing through the end of the Cold War, the US 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 lead and directed national
intelligence collection activities under authorities found in Title 50. The Intelligence Community
components of the Department of Defense often collected foreign intelligence in response to

---

15 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, United States Senate, Committee on the Armed Services (Apr. 15, 2010) at 10.
national tasking under Title 50 authorities, but they also collected tactical intelligence for military commanders.\textsuperscript{16}

This disjointed US national security apparatus and authorities continues today and often forces an unnatural categorization of governmental operations. How a problem is defined often dictates which agency will direct and control the government’s response and under which authorities that response will be conducted. Which authorities are invoked dictates which congressional appropriations can be used to fund the government’s response and well as which congressional committee will be notified and exercise oversight over the Executive Branch’s actions.

Take, for example, a hypothetical cyber attack on a Department of Defense computer system. If the attack originated from within the United States, then the Department of Justice and its Federal Bureau of Investigation would be the lead agency to investigate and respond (prosecute the offender) to the attack. If the attack originated from the governmental computers of an adversary, then the Department of Defense and its National Security Agency would be the lead agency to investigate and respond to the attack. In the case of an attack by an adversarial government, a whole panoply of issues arise related to the type of attack and damage inflicted, the answers to which in turn give rise to a range of permissible responses. The range of permissible responses leads to the central issue of this paper: when would the US response be an intelligence activity and when would it be a military operation?

\textbf{II. Operational Authorities or Congressional Oversight?}

This question of whether a given action is an intelligence activity or a military operation is colloquially expressed as the “Title 10-Title 50 issue”. This issue dates to the National Security Act of 1947, but intensified after 9/11 in the wake of expanded authorities for US military forces to counter and combat transnational non-governmental terrorist organizations. Most recently, this issue came to the forefront of congressional concerns related to the establishment of US Cyber Command. But what exactly is the issue: does the law require that intelligence activities and military operations be strictly separated, or does this practice reflect the turf wars of congressional oversight committees?

\textsuperscript{16} Intelligence collection was further organized by source and lead agency. The Central Intelligence Agency was primarily responsible for human intelligence (HUMINT); the National Security Agency 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 Central Intelligence Agency 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.” \textit{Id.} at 50.
A. Presidential Power

The President’s authority to direct cyber intelligence activities or offensive cyber operations (cyberwarfare) against external threats resides in his Constitutional executive and commander-in-chief powers. The President is vested with executive power 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.” As chief executive, the President may “manage the business of intelligence in such a manner as prudence may dictate.” This includes the authority to secretly collect intelligence for reasons of national security. As Commander-in-Chief, the President may employ the military to protect the national interests of the United States.

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. Simply put, Congress decides how to resource the US military and when to formally declare war, while the President decides how to employ the military in furtherance of US national security objectives — subject always to constitutionally permissive constraints enacted by Congress and available funding.

This Constitutional separation or balancing of power between the President and Congress sparked intense debate almost immediately. Discussions of the President’s constitutional authority as Commander-in-Chief implicate “some of the most difficult, unresolved, and contested issues in constitutional law.” There are two obvious sides to this debate: those who favor “inherent” Presidential power, versus those who favor a Congressional check on “imperial” Presidential power. One scholar astutely observes that “[w]riters on the relative powers of the

17 The President is vested with Executive Power by Article II, Section 1 of the US Constitution; Section 2 adds Commander-in-Chief powers.

18 U.S. CONST. art. II § 1.

19 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. See Youngstown Sheet & Tube Co. et al v. Sawyer, 343 U.S. 579, 587 (1952). The President asserted 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.” Id.

20 John Jay, FEDERALIST PAPERS No. 64.

21 See, e.g., Chicago & S. Air Lines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948). 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.” Totten v. United States, 92 U.S. 105, 106 (1876).


23 Curtis A. Bradley and Jack L. Goldsmith, Congressional Authorization and the War on Terrorism, 118 HARVARD L. REV. 2047, 2051 (May 2005).
presidency versus the Congress almost invariably lapse into advocacy when they comment on the textual, historical or functional bases of war powers.”

Those who favor presidential powers in the realm of national security point to the President’s enumerated powers, namely the “executive 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’ power of the purse and power to formally declare war.

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, on the other hand, 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.” These advocates, mostly law professors and members of Congress, 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.”

While reviewing two opposing books on Presidential war powers, Professor Jack Goldsmith brilliantly 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.” 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 rough way, the Framers’ original design.” Goldsmith concludes:


26 Fisher, supra note 50, at 11.


28 Id.
“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.”

B. Statutory Authorities

Constitutional debates over Presidential power aside, the President leads a national security apparatus established, funded and overseen by Congress. While our analysis of Presidential authority to conduct cyber intelligence activities and operations begins with Constitutional powers, it continues through the President’s subordinates who act under statutory or delegated authorities.

The office of Secretary of Defense is established in Title 10 of the US Code. The Secretary of Defense exercises “authority, direction and control over the Department of Defense” subject only to “the direction of the President” and provisions of the National Security Act of 1947. Title 10 recognizes that the powers and responsibilities assigned to the Secretary of Defense inherently include some intelligence authorities, while additional intelligence responsibilities are explicitly assigned to the Secretary of Defense by Title 50 and Presidential order. Executive Order 12333 assigns the Secretary of Defense as the Executive Agent of the US government for signals intelligence activities, which includes cyber intelligence activities. The Secretary of Defense may “perform any of his functions or duties, or exercise any of his powers through, or with the aid of, such persons in, or organizations of, the Department of Defense as he may designate” unless otherwise prohibited by law.

Cyber operations conducted by US government personnel against targets outside of US borders will be conducted by either the National Security Agency or US Cyber Command. The National Security Agency was established in 1952 by Presidential order pursuant to his commander-in-

---

30 Id.


35 10 U.S.C. §113(d).
chief authorities. The National Security Agency is part of the Department of Defense and an element of the Intelligence Community. The National Security Agency is the lead US agency for signals intelligence. The National Security Agency may provide technical assistance and expert personnel for use by any department or agency of the US government, or to support local law enforcement or other civil authorities.

US Cyber Command is a subordinate unified command under US Strategic Command and was established by the Secretary of Defense pursuant to his Title 10 authorities. As a combatant command, US Strategic Command receives its authorities from Title 10 and reports directly to the Secretary of Defense. US Strategic Command is the lead commander for information operations, which includes cyber operations. US Cyber Command operates under authorities delegated by US Strategic Command with the consent of the Secretary of Defense and President.

The same person, currently General Keith Alexander, leads both the National Security Agency and US Cyber Command. Accordingly, cyber operations could be conducted by the same technical experts regardless of whether the cyber operation is an intelligence or military activity. Just as the Secretary of Defense possesses authorities under both Title 10 and Title 50, so too does General Alexander as Director of the National Security Agency and Commander of US Cyber Command.


37 See, e.g., 10 U.S.C. §§ 192, 193, 194, 201, and 50 U.S.C. §403-5. See also 10 U.S.C. §201 and 50 U.S.C. §403-6, which require the Secretary of Defense to obtain the concurrence of the Director of National Intelligence before appointing an individual to become Director of the National Security Agency.

38 Executive Order 12333 (1981) as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008) at 20; 50 U.S.C. §403-5. Executive Order 12333 directs the National Security Agency to: “Establish and operate an effective unified organization for signals intelligence activities … No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director [of National Intelligence]. … Provide signals intelligence support…for the conduct of military operations.”

39 Executive Order 12333, supra note 30, at para. 2.6.


41 10 U.S.C. §§ 161, 162, 164, 165, 166, 166a, 166b, and 168. It should be noted that as a practical matter, the Commander of US Strategic Command communicates with the Secretary of Defense via the Joint Staff. The Chairman of the Joint Chiefs of Staff is not technically or legally in the chain-of-command; his legal 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.

This simultaneous exercise of separate statutory authorities is not unique to cyber activities, nor does it pose a threat to the lawful exercise of command and control over Department of Defense personnel. Title 10 and Title 50 are complementary, mutually-reinforcing authorities, not mutually-exclusive authorities. Indeed the “blending” of legal authorities and capabilities under General Alexander is precisely what is required to integrate US cyber operations.

C. Congressional Oversight

Congressional oversight is the primary challenge faced by the Department of Defense when simultaneously exercising Title 10 and Title 50 authorities. Intuitively, military activities executed under authorities found in Title 10 should be reported to the House and Senate Armed Services Committees, while intelligence activities executed under authorities found in Title 50 should be reported to and overseen by the intelligence committees. In practice, there is not always a clear distinction between acts that constitute military activities or intelligence activities as they may be authorized under both Title 10 and Title 50 — especially with respect to military intelligence activities. Furthermore, intelligence activities carried out by an element of the Intelligence Community may be 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 the Department of Defense and matters relating to “the common defense”.

Defense authorization bills originate in the armed services committees where they must be approved before consideration by the full Senate or House. Problems arose in the wake of 9/11 as the Department of Defense 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 — creating clashes with the Executive Branch and debates over appropriate congressional oversight.

Congressional oversight of intelligence activities is considerably more complex. The National Security Act of 1947, which created the Central Intelligence Agency, 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 New York Times reporter Seymour Hersh that US intelligence agencies engaged in domestic spying. The Church Committee’s subsequent investigation “did nothing less than revolutionize America’s attitudes toward intelligence supervision.”

The Senate established its Select Committee on Intelligence (SSCI) in 1976 and the House followed suit a year later with its Permanent Select Committee on Intelligence (HPSCI). The era


of benign neglect was over, replaced instead by dynamic if often dysfunctional congressional oversight. In 1980 Congress mandated for the first time that the Director of Central Intelligence and the heads of all other US departments and agencies “involved in intelligence activities” keep the intelligence committees “fully and currently informed of all intelligence activities.” 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.46

The intelligence committees exercise broad oversight of the intelligence community. They exercise exclusive authorizing powers for the Central Intelligence Agency, the Director of National Intelligence (formerly the Director of Central Intelligence) and the National Intelligence Program.47 They share jurisdiction of Department of Defense intelligence components with the Senate and House armed services committees.

The jurisdictions of the Senate and House intelligence committees are nearly identical with two significant differences: HPSCI uses a much broader definition of intelligence activities and adds oversight of “sources and methods”.48 SSCI 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.”49 The House gives “intelligence and intelligence-related activities” what seems to be an 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


47 The National Intelligence Program is “all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.” 50 USC §401a.

48 Authority to “review and study on an exclusive basis the sources and methods of entities” in the intelligence community was added in January 2001. Sources and methods is a catch-all phrase used by the intelligence community to elude to how and from whom information is gathered. House Rule 3(l), added by H.Res. 5, 107th Cong., January 3, 2001.

defense, foreign policy, national security, or related policies of the United States and other activity in support of the collection, analysis, production, dissemination, or use of such information.”

Thus, the House of Representatives via a rule change gave HPSCI oversight of “intelligence-related activities” including “tactical intelligence” and other military information collection activities for which congressional notification is not statutorily mandated. This could 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 also 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 with the defense subcommittees of the House and Senate Appropriations Committees.”

The 9/11 Commission recognized how “dysfunctional” this arrangement is in practice and recommended the establishment of a single joint intelligence committee with

50 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 (“findings”) requirements for covert actions. Executive Order 12333 defines intelligence activities as “all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.” One source of confusion springs from Title 50’s definition of “national intelligence”, which causes some to opine that “national intelligence” is distinguishable and exclusive of military intelligence. (See 50 U.S.C. § 401a(5)) 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. (See 50 U.S.C. § 403-5(a) & (b)) More accurately, Title 10 should be read as clarifying roles and responsibilities within the Department of Defense, while Title 50 clarifies roles and responsibilities within the intelligence community — with explicit recognition that the Secretary of Defense has statutory roles and authorities under both Title 10 and 50. Executive Order 12,333 then clarifies this by directing the Secretary of Defense to collect intelligence for both his department and the intelligence community writ large. US military doctrine further erodes any distinction between tactical, operational and strategic: “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.” US DEPARTMENT OF DEFENSE, JOINT PUBLICATION 3-0, DOCTRINE FOR JOINT OPERATIONS I-1 (Sep. 10, 2001).

51 Jennifer Kibbe, Congressional Oversight of Intelligence: Is the Solution Part of the Problem?, 25 INTELLIGENCE AND NATIONAL SECURITY 24-49, 29-30 (Feb. 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”.

14
authorizing and appropriating authorities.\textsuperscript{52} Congress has not seen fit to enact this recommendation.

Intelligence committee oversight is further weakened by their failure to enact an intelligence authorization bill for the past five 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.”\textsuperscript{53} Congress meets this “specifically authorized” provision through the use of a catch-all provision inserted into the defense appropriations acts.\textsuperscript{54} 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.

\section*{III. Intelligence Activities or Military Operations?}

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 division of congressional oversight 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 the activities to be intelligence activities or military operations.


\textsuperscript{53} 50 U.S.C. §414.

\textsuperscript{54} The catch-all provisions read similar to this one for fiscal year 2009:

\begin{quote}
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.
\end{quote}

As illustrated by Figure 1, the congressional intelligence committees exercise oversight of intelligence activities, while the armed services committees exercise oversight jurisdiction over military operations. The jurisdictional boundaries of congressional oversight are not synchronized 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 the Department of Defense to conduct covert action.  

The question of whether a cyber activity is an intelligence activity or a military operation 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 examine the distinctions between intelligence activities and military operations. When is the cyber activity intended to merely collect information versus when is it preparing for offensive cyber operations? The existence of a Secretary of Defense approved Execute Order directing military operations will decisively answer this question. While our analysis could end here as a legal matter, we will nonetheless examine why operational preparation of the

---

55 “No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective.” Exec. Order 12,333, para. 1.7(a)(4) (as amended, 2008).
environment is a traditional military activity, and not an intelligence activity. We will see why even unacknowledged operations by military personnel under military command and control are not covert action.

A. Moving From Information Collection to Preparing the Environment

The Secretary of Defense is authorized by law and executive order to conduct intelligence activities in cyberspace. This authority is grounded in his Title 10 authorities as head of the Department of Defense (10 USC §113), his inherent Title 10 intelligence authorities (10 USC §137), his specified Title 50 intelligence authorities (50 USC §403-5) and his delegated authorities contained in Executive Order 12333 and elsewhere. Specifically, Executive Order 12333 appoints the Secretary of Defense as Executive Agent for signals intelligence, which includes cyber intelligence activities. Executive Order 12333 assigns the National Security Agency, an element of the Department of Defense and the Intelligence Community, as the lead agency for cyber intelligence activities.

The Secretary of Defense may instruct the Director of the National Security Agency to carry out cyber intelligence activities in response to national intelligence requirements, or to meet the cyber intelligence needs of the Department of Defense. When the National Security Agency conducts cyber intelligence activities in response to national intelligence requirements, it does so primarily under Title 50 authorities (50 USC §403-5(b)(1)) and pursuant to priorities and needs determined by the Director of National Intelligence (50 USC §403-1(f)). When the National Security Agency conducts cyber intelligence activities to fulfill intelligence requirements of the Department of Defense, it conducts those cyber intelligence activities under Title 50 authorities (50 USC §403-5) and Title 10 authorities (e.g., 10 USC §113 and 10 USC §164) as well as delegated authorities from the President and Secretary of Defense. These cyber intelligence activities are part of a foreign intelligence program and are subject to congressional intelligence oversight and are reported to the intelligence oversight committees. The distinguishing feature of these cyber intelligence activities, for our purposes here, is that their intent is merely to collect knowledge and understanding of foreign cyber networks.

Elements within the Department of Defense may not go beyond merely gathering information in cyberspace, such as making initial preparations for future offensive operations, unless an Execute

56 General Alexander told the Senate Armed Services Committee that US Cyber Command, a subordinate unified command of US Strategic Command, was assigned missions (by the President through the Secretary of Defense and the Commander of US Strategic Command) that include: “integrating cyberspace operations and synchronizing warfighting effects across the global security environment … directing global information grid operations and defense; executing full-spectrum military cyberspace operations; [and] serving as the focal point for deconfliction of DOD offensive cyberspace operations ….” The President, through the Secretary of Defense, assigned these missions to US Strategic Command, which then delegated them with the concurrence of the President and Secretary of Defense, to US Cyber Command. US Strategic Command receives its statutory authorities to carry out assigned missions from Title 10 (10 USC §164), which it delegates in this instance to US Cyber Command.
Order is issued by the Secretary of Defense with the approval of the President. Preparing foreign networks for cyber operations is a military operation conducted under Title 10 authorities and is subject to oversight by the armed services committees. Two key characteristics distinguish military cyber operations from cyber intelligence activities: 1) the existence of a Secretary of Defense authorized Execute Order, and 2) execution under military command and control.

The preceding two-part test for distinguishing between intelligence activities and military operations is straightforward, yet it also irritates the intelligence committees. Members of SSCI and HPSCI have repeatedly expressed frustration over the past twenty years with what they see as the Department of Defense’s deliberate side-stepping of their oversight by renaming intelligence activities as “operational preparation of the environment” (OPE). These congressional concerns are generally raised in the context of human intelligence activities, but are apparent in the questions submitted to General Alexander prior to his confirmation as well.

In its report accompanying the Intelligence Authorization Act for 2010, HPSCI criticized the Department of Defense for frequently labeling its clandestine activities as operational preparation of the environment “to distinguish particular operations as traditional military activities and not as intelligence functions” and, implicitly, escape intelligence oversight. HPSCI opined that this practice made the distinction all but meaningless as the Department of Defense “has shown a propensity to apply the OPE label where the slightest nexus of a theoretical, distant military operation might one day exist.” HPSCI argues that this practice obfuscates the military operations from congressional oversight, yet oversight of OPE is in fact exercised by the armed services committee as evidenced by the content of the questions posed by the Senate Armed Services Committee to General Alexander.

---

57 10 USC §164(b). The National Command Authority exercises authority and control of the military through a single operational chain of command: from the President, through the Secretary of Defense, directly to the commanders of combatant commands for missions and forces assigned to their commands.

58 See General Alexander’s answers, supra note XX, at 15i, 15j, and 20a. General Alexander: “Military actions in cyberspace done to prepare the environment for possible cyber attack are authorized through SECDEF Execute Orders and reportable to the Armed Services Committees.”


60 House Permanent Select Committee on Intelligence, Report Accompanying the Intelligence Authorization Act for Fiscal Year 2010, 111th Congress, 2nd Session (Jun. 25, 2009), at 10. 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 USC §413, which pre-authorizes intelligence appropriations.

61 Id. at 11.
The issuance of an Execute Order is no mere technically or simple formality. 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.”\textsuperscript{62} Execute Orders are typically preceded by Planning Orders and a planning phase, so the Execute Order rightfully signals the transition from planning to operations.\textsuperscript{63} The Execute Order directs the execution of an approved military course of action. As such, it is also the appropriate signal that efforts have transitioned from merely collecting information to the commencement of military operations.

**B. Why Operational Preparation of the Environment is Not Covert Action**

A fundamental concern of the intelligence committees is that the Department of Defense’s clandestine activities labeled as operational preparation of the environment “carry the same diplomatic and national security risks as traditional intelligence-gathering activities.”\textsuperscript{64} 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 the Department of Defense is skirting the formal Presidential approval and reporting requirements for covert action by simply naming the activities as operational preparation of the environment.\textsuperscript{65}

A year after its creation by the National Security Act of 1947, the National Security Council issued NSC Directive 1012 — setting forth a policy of containment of the Soviet Union and redefining covert action. 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 underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous

\textsuperscript{62} Joint Publication 5-0, Joint Operation Planning (Dec. 26, 2006) at GL-11 and I-25

\textsuperscript{63} 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.

\textsuperscript{64} HPSCI Report, supra note 56, at 11.

\textsuperscript{65} See Nomination of General Michael V. Hayden USAF to be Director of the Central Intelligence Agency, Hearing Before the Senate Select Committee on Intelligence, 109th Cong., 2d Sess. (May 18, 2006) at 26-7. Leon Panetta, Director of Central Intelligence and former congressman, echoed these concerns in answers provided to SSCI following his confirmation hearing. In response to a question asking him to distinguish between covert action and operational preparation of the environment, Director Panetta answered: “I am concerned 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.” Questions for the Record, Nomination of the Honorable Leon E. Panetta, available at http://intelligence.senate.gov/090205/panetta_post.pdf.
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 US government actions for over forty years.

Congress defined covert action for the first time in 1991 following the Iran-Contra affair. Covert action is “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.” This definition was included in the Intelligence Authorization Act for 1991 and the Conference Report stressed that Congress did not intend for the definition to expand or contract previous definitions of covert action; the intent was simply to “clarify the understandings of intelligence activities that require Presidential approval and reporting to Congress.” The Conference Report further emphasized that the “definition of ‘covert action’ applies only to activities in which the role of the United States Government is not intended to be apparent or to be acknowledged publicly.”

After defining covert action, Congress next listed several activities that, in the words of the Conference Report, “do not fall within the definition of covert action.” These exclusions are:

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 US government.

While several of these exclusions could apply to cyber activities depending on the context and actors involved, our analysis will focus on traditional military activities as this is the exclusion applicable to operational preparation of the environment.

---

66 National Security Council Directive 1012 (June 1948) as quoted in GREGORY F. TREVERTON, INTELLIGENCE FOR AN AGE OF TERROR 210 (2009). Originally drafted by George Kennan, then director of the State Department’s Policy Planning Staff, Treverton states that “NSC 1012 was the turning point for covert action, expanding it from propaganda to direct intervention.”

67 Id.

68 10 USC §413b.


70 Id. 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.”
The Conference Report provides crucial insight into what Congress intended to include within the term “traditional military activities”:

The conferees note that "traditional military activities" and "routine support" to such activities do not fall within the definition of covert action. 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 control of a military commander should not be considered as "traditional military activities."

The Conference report sets forth a four-part test to determine whether an activity is a traditional military activity. The activity must be: 1) conducted by US military personnel, 2) under the direction and control of a US military commander, 3) preceding and related to anticipated hostilities or related to ongoing hostilities involving US military forces, and 4) the US role “in the overall operation is apparent or to be acknowledged publicly.”

Two points deserve emphasis. First, traditional military activities need not be acknowledged publicly so long as the US role in the overall operation will be apparent or acknowledged. This fact is apparent from the actual statutory language and construction and is emphasized by the Conference Report. This means, for example, that the US military could conduct unacknowledged cyber operations under Title 10 authorities so long as those cyber operations were met the four criteria set forth in the preceding paragraph. Secondly, when the activities in question precede anticipated hostilities, the National Command Authority (President and Secretary of Defense) must approve the activities and operational planning for hostilities. As we saw previously, the approval for operational preparation of the environment is contained in an Execute Order, while approval for operational planning is typically contained in a Planning Order.71 The Secretary of Defense must approve the shift from planning to operations.

The Conference Report does add a caveat of sorts with respect to “activities undertaken well in advance of a possible or eventual U.S. military operation.” Whether such activities “constitute covert action” will depend in most cases on whether they constitute ‘routine support’ to such an operation.”72 The Conference Report then references the explanation of “routine support”

71 See Joint Publication 5-0, Join Operation Planning (Dec. 26, 2006).

72 Conference Report, supra note 66.
contained in SSCI’s Report accompanying the Senate version of the Intelligence Authorization Act for 1991. The Senate Report defines routine support to be “unilateral U.S. activities to provide or arrange for logistical or other support for U.S. military forces in the event of a military operation that is to be publicly acknowledged.”\footnote{73} Examples of routine support include “caching communications equipment or weapons,” leasing or purchasing residential or commercial property to support an aspect of an operation from unwitting sources, or “obtaining currency or documentation for possible operational uses.”\footnote{74}

The Senate Report then adds this limitation on what it considers to be routine support:

The Committee would regard as "other-than-routine" support activities undertaken in another country which 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 efforts to influence foreign nationals of the target country concerned to take certain actions in the event of a U.S. military 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.\footnote{75}

It is not clear whether the Executive Branch accepts this caveat on routine support as controlling,\footnote{76} nor does the caveat makes sense in light of the definition of traditional military activities. If the examples provided by SSCI as “other-than-routine” support activities meet the four-part test for traditional military activities, then they are military operations and not covert action. There would then be no need to look further at routine support. Rather, the examples listed are classic examples of unconventional warfare activities.\footnote{77} Given that these activities are conducted outside the United States it is difficult to imagine them being conducted absent an Execute Order. This caveat, then, would as a practical matter only apply to non-military personnel.

\footnote{73}{S. REP. NO. 102-85 (1991)(Conf. Rep.).}
\footnote{74}{Id.}
\footnote{75}{Id.}
\footnote{76}{Statements in committee reports 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."). In other words, committee reports can be helpful in explaining congressional intentions and definitions, but they can hardly be construed to impose more demanding or constraining requirements than those contained in the actual statutes.}
\footnote{77}{See US Department of Defense, Joint Publication 3-05, Doctrine for Joint Special Operations Forces II-7 (Dec. 17, 2003); US Army Field Manual 3-05.130, Army Special Operations Forces Unconventional Warfare 1-2 (Sep. 2008).}
IV. Concluding Analysis

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.” The Report provides this helpful illustration:

![Box 1—Cyberattack versus Cyberexploitation](image)

Source: NATIONAL RESEARCH COUNCIL.

This illustration is a helpful starting point, but its simplistic separation of Title 10 and cyber attack in one column, while placing Title 50 and cyber exploitation in another column, belies the stove-piped 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.

---

78 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.).
A. Intelligence Activities

Likely cyber exploitation activities could include mapping and scanning networks to collect information and identify vulnerabilities, hacking into networks to collect information, or installing malware or spyware that collects information or installs a back-door. The primary purpose of these activities is to collect information or intelligence. When these activities are conducted under the National Intelligence Program, or pursuant to the direction of the Director of National Intelligence, they are intelligence activities conducted under Title 50 authorities. These intelligence activities would be reported to the intelligence committees.

If these same cyber exploitation activities were conducted by US Cyber Command or service intelligence elements pursuant to an Execute Order approved by the Secretary of Defense, then these activities would be military operations conducted under Title 10 authorities. An Execute Order could be issued because the networks being exploited belong to the military of a nation with which the United States is at war, or they could belong to an enemy with which conflict is imminent. The activities could even be unacknowledged, so long the US role in the actual or imminent military operation was to be acknowledged.

Consider the following hypothetical scenario. Rogueland has been pursuing a nuclear weapons capability for several years in flagrant violation of international law (Nuclear Non-Proliferation Treaty) and numerous UN Security Council resolutions. Intelligence estimates vary, but the general consensus is that Rogueland does not have a nuclear weapons capability and, at its current rate of progress, such a capability is 4-6 years off. The US military commander whose area of responsibility includes Rogueland, believes Rogueland will continue working towards obtaining a nuclear weapons capability. The commander is convinced the US President should have a viable military option to destroy Rogueland’s nuclear weapons capability before it becomes operational. His planning team proposes using special operations forces to enter Rogueland, infiltrate its military command and control networks, collect intelligence on Rogueland’s nuclear capabilities, and if directed ultimately sabotage those capabilities. The planners envision using US military forces or local surrogates to gain physical access to the process control systems for Rogueland’s power generation and distribution and install devices on the SCADA-related network jacks and switches, thereby giving US forces the ability to bypass security on the control software and fully control Rogueland’s power network.

This scenario conjures up the intelligence committee’s worst fears. The military operation proposed by the regional combatant commander could be justified as operational preparation of the environment, but that would require an Execute Order approved by the President. This begs the question, how could the President order military operations against another country without a

casus belli? Article 2(4) of the UN Charter prohibits the threat or use of force as a means to resolving interstate disputes, and Article 51 only recognizes the right of self-defense in response to an armed attack. The United States has consistently maintained the right to use force in anticipatory self-defense when an armed attack is imminent, but it defies logic to argue that the facts in this scenario give rise to an imminent threat. US intelligence estimates indicate Rogueland is 4-6 years away from a nuclear weapons capability; additionally, there needs to be some evidence of an imminent threat by Rogueland to use the weapon. Thus, while there is no explicit statutory requirement that Execute Orders be premised upon a legal use of force, it seems logical to infer such a prerequisite to Presidential approval. The President could, however, direct that these same activities be conducted by intelligence personnel as a covert action pursuant to the requirements of Title 50 and Executive Order 12333.

B. Military Operations

The United States is engaged in an ongoing conflict with an international terrorist organization known as The Base. The Base secretly operates from several countries, including Orangeland, where it plans and initiates attacks on American citizens and institutions worldwide. Orangeland is governed by a weak autocracy, which is fighting homegrown insurgents. Some insurgent groups are cooperating with The Base, which provides them with training and money in exchange for a safe haven in remote regions of Orangeland. The government of Orangeland, while not particularly friendly to the United States, has requested limited US military assistance in its fight against The Base. The United States does not wish to become embroiled in Orangeland’s simmering civil war, but does agree to deploy a small number of special operations forcers to Orangeland to train and advise government security forces in their fight against The Base.

Intelligence indicates The Base is using Orangeland as a key command and control hub: linking communications between cells in various countries, conducing recruitment, and disseminating propaganda. The Base relies heavily upon the internet for propaganda and recruiting, and operates from several internet cafes in Orangeland. The combatant commander whose area of responsibility includes Orangeland wants the special operations forces to collect intelligence on The Base while they are in Orangeland. He would like to send US soldiers in disguise into the internet cafes close to known The Base safe havens to install keystroke logging software on the computers, which would enhance efforts to collect intelligence on The Base and its operatives and contacts. The software would permit continued network access and intelligence collection after the special operations forces redeployed.

80 For the definitive explanation to date on when cyber attacks may rise to the level of an armed attack under Article 51, see Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUMBIA J. TRANSNATIONAL L. 887 (1999).
The activities proposed fall within the general category of cyber exploitation, yet if they are conducted pursuant to an approved Execute Order these activities would constitute a military operation under Title 10 authorities and not intelligence activities. Because the United States is in an armed conflict with The Base, an international terrorist organization, the President could authorize military operations against The Base wherever it is located.81 Similarly, the Secretary of Defense may approve the use of cyber attacks against The Base websites and other cyber targets. Again, these activities would not need to be individually acknowledged so long as US involvement in an ongoing military campaign against The Base is acknowledged.