ARTICLE

Traditional Military Activities in Cyberspace: The Scope of Conventional Military Authorities in the Unconventional Battlespace

Major Peter C. Combe II[*]

[*] Judge Advocate, United States Marine Corps. Presently assigned as Operational Law Attorney, International and Operational Law Branch, Judge Advocate Division, Headquarters Marine Corps. LL.M., 2015, The Judge Advocate General's School,; J.D., 2008, University of Houston; B.S., 2003 Cornell University. Previous assignments include Legal Services Support Section – National Capital Region, Marine Corps Base Quantico, Virginia, 2010-2014 (Deputy Officer in Charge, Legal Services Support Section, 2013-2014; Senior Defense Counsel, 2012-2013; Defense Counsel, 2011-2012; Trial Counsel, 2010-2011); Operational Law Attorney, International Security Assistance Force/United States Forces-Afghanistan, 2013; Platoon Commander, Officer Candidates School, Marine Corps Base Quantico, Virginia, 2011. Member of the State Bar of Texas. This article was submitted in partial completion of the Master of Laws requirements of the 63d Judge Advocate Officer Graduate Course.

Table of Contents

Thus, those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations.[1]

Introduction

The year is 2020 and the United States sits squarely in the crosshairs of an enemy half a world away. The threat is as dangerous and sophisticated as any the nation has faced; however, the United States military is poorly postured to counter the threat. The dispute between China and Japan over the Senkaku Islands[2] has continued to escalate since the discovery of vast undersea energy resources in the late 1960s.3 Chinese actions have included aggressive statements of undisputed sovereignty and shows of military force,[4] culminating in the establishment of a disputed Air Defense Identification Zone.[5] American military to military engagement and combined exercises with Japan have only increased tensions between China and the United States.[6]

Most problematic for the United States is the negative characterization of American and Japanese forces in domestic and international media. Reports and photographs have surfaced purporting to show the aftermath of a combined American and Japanese attack on unarmed Chinese fishing vessels in the East China Sea.[7] Chinese and international news outlets have continued to report on

---

[1] SUN TZU, THE ART OF WAR 79 (Samuel B. Griffith trans., Oxford Univ. Press 1963).

[2] LARRY M. WORTZEL, THE CHINESE PEOPLE'S LIBERATION ARMY AND INFORMATION WARFARE, at X (Strategic Stud. Inst., U. S. Army War C. Press, Mar. 2014). The Chinese name for these disputed islands is "Diaoyu." *Id.*

[3] Jean-Marc F. Blanchard, The U.S. Role in the Sino-Japanese Dispute over the Diaoyu (Senkaku) Islands, 1945-1971, 161 CHINA Q. 95, 98 (Mar. 2000).

[4] *See generally* Daniel Tretiak, *The Sino-Japanese Treaty of 1978: The Senkaku Incident Prelude*, 18 ASIAN SURV. 1235 (Dec. 1978). During the 1978 Senkaku Islands incident, over 80 Chinese vessels (ostensibly fishing boats), armed with weapons including machine guns, approached the Senkaku islands, in direct challenge to Japanese claims of territorial sovereignty over the islands. *Id.*

[5] Madison Park, *Why China's New Air Zone Incensed Japan, U.S.*, CNN WORLD NEWS (Nov. 27, 2013), http://www.cnn.com/2013/11/25/world/asia/china-japan-island-explainer/index.html.

[6] Outside of the context of the hypothetical example, the U.S. military is also conducting combined military operations with other nations that contest Chinese claims in the South China Sea, East China Sea, and Yellow Sea. *See, e.g.*, Carla Babb, *U.S. Announces Joint Patrols With Philippines in South China Sea*, VOICE OF AMERICA (Apr. 14, 2016), http://www.voanews.com/content/us-announces-joint-patrols-with-philippines/3285277.html; Jeremy Page, Jay Solomon, & Julian Barnes, *China Warns U.S. as Korea Tensions Rise*, WALL STREET JOURNAL (Nov. 26, 2010), http://www.wsj.com/articles/SB10001424052748704008704575638420698918004.

[7] Similar falsified reports of alleged Ukrainian atrocities surfaced in the days preceding the Ukrainian election in October 2014. These reports involved the use of digitally altered photographs, which "hackers" were able to project onto digital billboards in Kiev before the election. Russian state media outlets continued to report on the story. *See, e.g.*, Carl Schreck, *Ukraine Unspun: Chechnya War Pic Passed off as Ukraine Atrocity by Hackers, Russian TV*,

the alleged attack, while outlining the efforts made by the Chinese People's Liberation Army Navy (PLAN) to deescalate the confrontation, and to ensure peace and freedom of commercial shipping and air travel in the area.[8]

Meanwhile, American newspapers have published pieces describing Chinese legal claims over the Senkaku Islands, and denouncing American and Japanese efforts in the East China Sea as illegitimate and provocative.[9] Chinese President Xi Jinping[10] has published an open letter to the American people,[11] imploring America's leaders to cease their aggressive actions in the East China Sea, and to take steps to accommodate China's "peaceful rise" to superpower status.[12] President Jinping also informs American voters that China's "peaceful rise" is inevitable, and is in the best interest of global prosperity. Finally, Chinese cyberspace operations have compromised non-secure military networks and public-facing Department of Defense websites. These attacks have included data corruption,[13] distributed denial of service attacks,[14] and publication on DOD websites of the same news stories justifying Chinese actions, and denouncing U.S. and Japanese efforts as illegitimate and criminal.[15] The PLA has also attacked

---

RADIO FREE EUR. RADIO LIBERTY (Oct. 27, 2014), http://www.rferl.org/content/russian-media-propaganda-ukraine-conflict-chechnya/26660126.html.

[8] Reports indicate that state-owned China Central Television operates overseas subsidiaries in the native language that toe the Communist Party line and portray the People's Liberation Army as "contributing to international peace and Stability." WORTZEL, *supra* note 3, at 32.

[9] China has used similar methods in the past to insert paid advertisements, which look like news articles, praising single party rule in China, into at least two major American newspapers. U.S.-CHINA ECON. AND SECURITY REV. COMM'N, 2011 REPORT TO CONGRESS 322–23 (Gov't Prtg. Office, 2011).

[10] President Xi Jinping assumed duties as the President of China in March of 2013. *China new leaders; Xi Jinping heads line-up for politburo*, BBC NEWS CHINA (Nov. 15, 2012), http://www.bbc.co.uk/news/world-asia-china-20322288. The Chinese President serves for no more than two five-year terms. XIANFA art. 60, § 1; art. 79, § 2 (1982) (China).

[11] *Cf.* Vladimir V. Putin, *A Plea for Caution From Russia*, N.Y. TIMES (Sept. 11, 2013), http://www.nytimes.com/2013/09/12/opinion/putin-plea-for-caution-from-russia-on-syria.html.

[12] *Cf.* Yang Jiechi, State Councilor of China, *Statement at the Opening Session of the 51st Munich Security Conference*, CHINA DAILY USA (Feb. 7, 2015), http://usa.chinadaily.com.cn/china/2015-02/07/content_19517526.htm; State Council Info. Office, *China's Peaceful Development Road*, PEOPLE'S DAILY ONLINE (Dec. 22, 2005), http://en.people.cn/200512/22/eng20051222_230059.html.

[13] These types of attacks are within the scope of China's cyber strategy, and have apparently been carried out against the Japanese Diet to compromise Japanese Parliamentary data. Monicka Chansoria, *Defying Borders in Future Conflict in East Asia: Chinese Capabilities in the Realm of Information Warfare and Cyber Space*, 26 J. E. ASIAN AFF. 105, 115, 122 (Spring/Summer 2012).

[14] China has also apparently overloaded South Korean servers, resulting in a distributed denial of services attack in 2009. *See, e.g.*, *id*. at 122. Distributed denial of services is essentially an offensive cyber operation which seeks to degrade, often to the point of shutting down, particular internet domains, servers, or other computer based systems and communications. *See, e.g.*, *Understanding Denial of Service Attacks*, UNITED STATES COMPUTER EMERGENCY RESPONSE TEAM (Nov. 2009), https://www.us-cert.gov/ncas/tips/ST04-015.

[15] Outside of this hypothetical, this vulnerability in service-maintained public domain websites has already been exploited. *See, e.g.*, Julian E. Barnes, *Syrian Electronic Army Hacks Marines*

United States Pacific Command (PACOM) social media websites, resulting in a significant black eye for U.S. information efforts.[16] As a result of these continuous losses in the information space, the Pentagon and the Japanese Ministry of Defense have been on the defensive, responding with a series of reactive measures to counter rapidly degrading public opinion in both the domestic and international communities. While the military has developed plans and capabilities to respond, the lack of clear authorities to conduct cyberspace operations hampers U.S. initiative, and degrades the effectiveness of any response.

The United States cyber arsenal provides unparalleled capabilities, but the byzantine approval and oversight regimes of domestic law contribute to significant confusion and disagreement over which agencies have the responsibility to conduct such operations. This morass of legal and policy requirements hampers United States responsiveness and impedes the U.S. ability to engage adversaries proactively in the cyber domain. This confusion stems from vague definitions, and from turf wars between executive agencies. One of the most contentious areas involves unacknowledged, or covert, U.S. activities in cyberspace.

"Covert activities" are unacknowledged actions by the United States Government that are undertaken to "influence political, economic, or military conditions abroad."[17] Such activities are subject to formalistic decision-making and oversight rules.[18] The President or Secretary of Defense must approve all covert activities that are not in support of ongoing hostilities.[19] Furthermore, the executive must provide detailed reports on covert activities to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence (SSCI and HPSCI, respectively).[20]

There are a number of exceptions to the usual reporting and decision-making rules for covert activities, none provoking more confusion and argument than the exception for "traditional military activities" (TMA).[21] The current TMA framework is inadequate in light of current operations in cyberspace, and a blurring of distinctions between military and intelligence communities. This

---

Website, WALL ST. J.: WASH. WIRE BLOG (Sept. 2, 2013), http://blogs.wsj.com/washwire/2013/09/02/syrian-electronic-army-hacks-marines-website/.

[16] *Cf.* Jose Pagliery et. al., *CENTCOM Twitter Account Hacked, Suspended*, CNN (Jan. 12, 2015), http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/index.html. While the compromise of CENTCOM's Twitter and Youtube accounts do not represent breaches of either secure or non-secure military networks, the messaging victory for the Islamic State is in many ways independent of the reality that this represents a minimal (if any) security breach of U.S. military networks.

[17] Intelligence Authorization Act, Fiscal Year 1991 § 503(e), 50 U.S.C. § 3093(e) (1991).

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

confusion hampers U.S. and DOD initiative in cyberspace, which is a significant handicap to U.S. military operations in cyberspace in the face of Chinese military organization and doctrine. Therefore, a new TMA framework is required to address current military roles and responsibilities in cyberspace.

The following provides an analysis of the statutory framework for decision-making and congressional oversight of unacknowledged military information support operations (MISO)[22] in cyberspace, and the extent to which those operations are either "covert activities" or TMA. Congress and other agencies dispute the scope of TMA. This opposition stems in part from the military's frequent conduct of intelligence and information operations that are remote in time and space from the ongoing hostilities with which they are associated. There is still no binding definition for what constitutes a TMA aside from three ill-defined elements in the legislative history of the covert action statute. These elements require that a TMA be (1) commanded by a military commander, (2) conducted by military personnel, and (3) pursuant to ongoing or anticipated hostilities in which the U.S. role is apparent or intended to be acknowledged. [23] The conduct of unacknowledged military activities in cyberspace requires a clear and concise analytical framework to properly identify which activities in cyberspace are TMA.

Presented first is a brief overview of Chinese cyber doctrine, and its operational focus on the United States. Next is a description of the current decision-making and oversight frameworks imposed on the executive with respect to covert or unacknowledged operations and the exception for TMA. This discussion will also identify the deficiencies in the TMA framework. The statutory and policy framework governing MISO, and cyberspace operations in domestic law are discussed, along with an acknowledgment of contentious issues in these types of operations, and the extent to which the uncertainty borne out of those deficiencies hamper U.S. initiative in cyberspace. The final section proposes a new TMA framework.

II. China's "Informatized" Revolution in Military Affairs

United States military operations in the Balkans and the first Gulf War served as a wakeup call to the Chinese military.[24] These American victories demonstrated two things to the People's Liberation Army (PLA): first, that information operations (IO) can provide a powerful advantage to the nation which employs them effectively;[25] and second, the extent to which China's own cyber

[22] Although primarily concerned with MISO, this analysis is applicable to the range of military operations. The analysis focuses on MISO operations as they are in a "gray area" between cyberspace operations that might have physical effects, and are thereby akin to traditional "kinetic operations," and cyberspace espionage that preferably would have no observable effects.
[23] S. REP. 102-85, at 44–48 (1991).
[24] WORTZEL, *supra* note 3, at 1.
[25] *Id.*

and information doctrines were lacking.[26] The PLA has continued to revise its cyberspace and information operations doctrines over the past two decades.[27]

The PLA established an incredibly well resourced and funded cyber warfare unit, Unit 61398.[28] Unit 61398 and other Chinese cyberspace operations units aggressively recruit university graduates with degrees in computer science-focused fields and strong English language skills.[29] Chinese cyberspace operations have been focused on English speaking countries—specifically the United States[30]—and have included cyber espionage efforts to collect data about high-end U.S. weapons systems from a number of defense contractors.[31] Chinese efforts are focused on bringing about a revolution in military affairs, which it views as a shift from "mechanized" warfare to one of "informatized" warfare.[32]

China developed Integrated Network Electronic Warfare (INEW) as the central doctrinal concept in "informatized" warfare.[33] A critical aspect of INEW is China's ability to win the information space, particularly against the U.S. in the cyber domain.[34] Cyberspace provides an attractive means for the PLA to combat an adversary with greater resources and technology for two main reasons. First, the PLA can operate with relative anonymity and impunity.[35] Second, cyberspace

---

[26] *Id.*

[27] M. Ehsan Ahrari, U.S. Military Strategic Perspectives on the PRC: New Frontiers of Information-Based War, 37 ASIAN SURV. 1163, 1169 (1997); WORTZEL, *supra* note 3, at 1.

[28] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 11 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. Mandiant compiled a detailed report on PLA Unit 61398, the PLA's premier cyberspace operations unit. *Id.*

[29] *Id.* at 11.

[30] *Id.* at 21.

[31] Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, WASH. POST (May 27, 2013), http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weaponssystem-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html. Among the U.S. defense contractors targeted were Boeing, Lockheed Martin, Raytheon, and Northrop Grumman. *Id.*

[32] TIMOTHY L. THOMAS, THE DRAGON'S QUANTUM LEAP: TRANSFORMING FROM A MECHANIZED TO AN INFORMATIZED FORCE 38-39 (U.S. Army Foreign Mil. Stud. Office, 2009); Chansoria, *supra* note 134, at 111.

[33] WORTZEL, *supra* note 3, at 10.

[34] *Id*. at 7–8. INEW has been described as a variation of the old Soviet era Radio-Electronic Combat (REC) "on Chinese steroids." *Id.* at 13. Essentially, the concept involves traditional tactical electronic warfare augmented by, and integrated with, cyberspace operations. *Id.* at 13–16. These operations in the information and electromagnetic domains are then combined with lethal strikes on satellite systems to cripple an adversary's Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), and precision strikes on traditional centers of gravity within areas of active combat operations. *Id.* at 13–14. For a discussion of Soviet-era REC, *see* DEF. INTELLIGENCE AGENCY, FUTURE SOVIET THREAT TO U.S. AIRBREATHING RECONNAISSANCE PLATFORMS: A SPECIAL DEFENSE INTELLIGENCE ESTIMATE 4 (1986).

[35] Office of the Nat'l Counterintelligence Exec., Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 1 (2011).

provides a low cost of entry, and ready availability of capabilities as compared to more conventional military technologies.[36]

Cyberspace is only the medium; the other aspect of Chinese doctrine is the information, or messaging, by which the PLA seeks to achieve effects. The General Political Department (GPD) serves as the primary agency responsible for Chinese messaging and propaganda.[37] The GPD's construct for influencing the information domain is called the "three warfares:"[38] (1) Public Opinion Warfare, (2) Psychological Warfare, and (3) Legal Warfare.

Public opinion warfare is waged through the domestic and international media, including state-owned media outlets abroad.[39] The objective of public opinion warfare is to sway domestic and international popular opinion in China's favor.[40] Psychological warfare seeks to degrade the morale of an adversary's military forces and civilian government officials.[41] Through legal warfare China attempts to be on the "cutting edge" of international law.[42] China makes aggressive legal claims, and backs these through shows of force and diplomatic action;[43] thereby attempting to garner the support of friendly governments, place powerful adversaries on the defensive, and cow weaker adversaries into acquiescence.[44]

The objective of the "three warfares" is to set conditions for the PLA to combat a technologically superior opponent through INEW,[45] with minimal fighting.[46] INEW doctrine is directly aimed at defeating U.S. military superiority in the event of a conflict over Taiwan, the South China Sea, or other Chinese interests.[47] The problem for the U.S. is that, while possessing unmatched capabilities in cyberspace and information operations, domestic legal authorities

---

[36] Chansoria, *supra* note 134, at 106.
[37] Larry Wortzel, *General Political Department and Evolution of the Political Commissar System*, *in* THE PEOPLE'S LIBERATION ARMY AS AN ORG.: REFERENCE VOL. 1.0 229–33 (James Mulvenon & Andrew Yang eds., 2002).
[38] WORTZEL, *supra* note 3, at 29.
[39] *Id.* at 30–32.
[40] *Id.* at 30.
[41] Mark A. Stokes, *The Chinese Joint Aerospace Campaign: Strategy, Doctrine, and Force Modernization*, *in* CHINA'S REVOLUTION IN DOCTRINAL AFFAIRS 271–74 (James Mulvenon and David Finkelstein eds., RAND Corp. 2002).
[42] *See, e.g.*, Peter Dutton, *Three Disputes and Three Objectives*, 64 NAVAL WAR COLL. REV. 43, 54 (2011); WORTZEL, *supra* note 3, at 30, 37–38. For instance, China has aggressively claimed sovereignty to the South China Sea, and all islands located therein. For a discussion of the history and legal merits of China's "nine-dash line" claim to the South China Sea, *see* N. Elias Blood-Patterson, *Smoke on the Water: The Role of International Agreements in the Philippine-Chinese Dispute of the South China Sea*, 46 N.Y.U. INT'L L. & POL. 1207, 1222–32 (2014).
[43] WORTZEL, *supra* note 3, at 37–38.
[44] *Id.* at 38.
[45] Krekel et. al., Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage 47–48 (2012).
[46] *See, e.g.*, SUN TZU, *supra* note 2, at 77.
[47] *See, e.g.*, KREKEL ET. AL., *supra* note 46, at 31; WORTZEL, *supra* note 3, at 27–28.

are unclear and the subject of significant contention. This friction hampers U.S. ability to proactively counter Chinese efforts in the cyber domain.

III. Muddying the Waters: Legal and Policy Schemes

A. *Covert Activities and the Traditional Military Activities Exception*

Covert action is "an activity 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."[48] However, the intent to acknowledge a specific action does not equate to an affirmative duty to either announce, or to actually acknowledge the U.S. role. [49] Thus, an unacknowledged military action is not "covert" if acknowledgment is intended at some point in the future.[50] This appears to be the case even if the discrete action is independent, and is not in support of some larger "overall" operation.[51]

This leads to a situation in which a particular action may never be announced, nor acknowledged upon request, yet would not be defined as covert action so long as it is either (1) in support of a larger acknowledged operation, or (2) acknowledgement is *intended* at some point in the future. Furthermore, this acknowledgment can take place after the successful completion of an action that might otherwise qualify as "covert," as in the instance of the raid that killed Osama bin Laden.[52] This raises questions of whether, when, and how the intent to acknowledge a specific action is captured, as well as what conditions must be satisfied before the action is acknowledged.[53]

Assuming that an action qualifies as covert, there are two requirements that are intended to ensure a balance between the separate powers of Congress and the President.[54] These two requirements are established by the covert action reporting statute. [55] The first is a decision-making requirement, and ensures

---

[48] 50 U.S.C. § 3093.

[49] Andru Wall, Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action, 3 HARV. NAT'L SECURITY J. 85, 130 (2011).

[50] 50 U.S.C. § 3093(e); S. REP. 102-85 at 46–47.

[51] *See, e.g.*, Robert Chesney, Computer Network Operations and U.S. Domestic Law: An Overview, 89 INT'L L. STUD. 218, 232 (2013).

[52] *See, e.g.*, Helene Cooper, *Obama Announces Killing of Osama bin Laden*, THE LEDE, N.Y. TIMES NEWS BLOG (May 1, 2011), http://thelede.blogs.nytimes.com/2011/05/01/bin-laden-dead-u-s-official-says/?_r=0. Despite the fact that then CIA Director Panetta exercised "overall command," thus disqualifying the raid from treatment as TMA, the U.S. acknowledgement (and apparent intent to do so) would mean that it does not satisfy the threshold definition of "covert action."

[53] There does not appear to be any specific guidance that identifies how and when the intent to acknowledge a specific independent action is expressed or preserved.

[54] 50 U.S.C. § 3093(a).

[55] 50 U.S.C. § 3093(e). The statute defines covert action, enumerates the TMA exception, and implements the presidential decision-making and congressional reporting requirements for covert

executive branch accountability for covert actions that pose the risk of political or diplomatic fallout abroad.[56] The second provides congressional oversight and democratic accountability where the President undertakes politically or diplomatically risky actions;[57] in particular, it allows Congress to exercise the "power of the purse." Furthermore, the statute establishes a number of exceptions to those normal reporting and decision-making rules.[58] The decision-making framework exists to ensure that a senior executive official remains informed of all unacknowledged actions that pose significant diplomatic risk.

For any covert action, the President must make a determination that "the action is necessary to support the identifiable foreign policy objectives of the United States, and important to national security."[59] While this ensures that there is deliberative thought in authorizing covert actions, the primary concern is to ensure that the President is accountable when a covert action has negative diplomatic consequences.[60] These findings must be reduced to writing prior to authorizing the action, and the President can only authorize actions that will take place, not those that already have taken place.[61] While this function ensures that the President may not later disavow knowledge of a covert action, this "check" only comes into play in the event a particular covert action attracts diplomatic or Congressional attention. Congress has also set up a mechanism by which covert actions are reported to the intelligence committees, thereby enabling congressional oversight.

---

actions. This statute was passed in 1991, and is in part a culmination of congressional response to the Church and Pike Committee reports on "the lessons of the 1970s." These reports exposed high-risk CIA activities, which often lacked proper oversight within the executive branch. The Church Committee Reports are a series of 14 congressional reports that expose various intelligence agency practices of the 1960s and 1970s. *See, e.g.*, FINAL REP. OF THE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. REP. 94-755 (1976) [hereinafter CHURCH REPORT]. The Pike Committee Report was never published; however, the Pike Committee was authorized to investigate illegal intelligence activities conducted by a number of federal agencies, including the CIA, NSA, and the FBI. *Investigation of Publ'n of Select Comm. on Intelligence Rep., Hearings Before the Committee on Standards of Official Conduct*, 94th Cong. 2 (1976) [hereinafter *Pike Report Investigation*]. While the report was never published, a subsequent congressional investigation looked into the unauthorized leak of a draft of the report to CBS news. *Id.* at 36.

[56] Robert Chesney, Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate, 5 J. NAT'L SECURITY L. & POL'Y 539, 540 (2012).

[57] *Id.* at 541.

[58] 50 U.S.C. § 3093(e); S. REP 102-85 at 44–48.

[59] 50 U.S.C. § 3093(a). The statute lists other requirements for the presidential determination. The finding must be in writing, unless time does not permit. In such cases, the determination will be reduced to written findings within 48 hours. The finding shall also specify the department or agency that will fund or participate in the activity and specify that all persons participating in the activity will follow CIA policy. As a general rule the President's determination cannot authorize or make findings on an action already taken.

[60] Chesney, Military-Intelligence Convergence, *supra* note 57, at 602; Chesney, Computer Network Operations and U.S. Domestic Law, *supra* note 52, at 223.

[61] 50 U.S.C. § 3093(a).

This oversight mechanism requires the Director, CIA to report certain information to the SSCI and the HPSCI.[62] First, the Director must keep the committees informed of all covert actions and provide details regarding all covert actions to Congress.[63] Second, the Director must furnish all material concerning covert actions to the congressional intelligence committees.[64] In theory, this allows Congress to use the "power of the purse" to check future similar covert actions, or ongoing covert action programs.[65] These decision-making and oversight requirements are not universal, as there are several exceptions to the covert action rules.[66] Among these are activities primarily designed to gather intelligence, traditional diplomatic or law enforcement activities, and traditional military activities (including routine support thereto).[67]

Perhaps the most important exception to the covert action definition is that for traditional military activities and routine support for those actions.[68] The statute does not define TMA; rather, the definition used by Congress and the President is found in the statute's legislative history.[69] Because the Senate Report specifically excludes activities to influence opinions and actions abroad from the definition of "routine support," these activities can only fit within the exception to the extent that they are TMA.[70] The Senate Report to the covert action statute identifies three elements, all of which must be met, for an action to qualify as TMA.[71] These elements require that a specific action be (1) commanded by a military commander, (2) conducted by military personnel, and (3) pursuant to ongoing or anticipated hostilities in which the U.S. role is apparent or to be acknowledged.[72] Some commentators recognize a fourth element requiring that an activity be one "traditionally" military in nature, or one that otherwise comports

---

[62] 50 U.S.C. § 3093(b).
[63] *Id.*
[64] *Id.*
[65] *See, e.g.*, JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 102 (2007) (indicating that the power of the purse is Congress' primary check on executive action).
[66] 50 U.S.C. § 3093(e).
[67] *Id.*
[68] *Id.*
[69] S. REP. 102-85 at 44–48.
[70] *Id.* at 47. The Senate Report intimates that "routine support" are unilateral U.S. actions, but that "routine support" does not include "clandestine effects [sic] to influence foreign nationals of the target country to support U.S. forces in the event of a 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." *Id.* While not specifically mentioning Military Information Support Operations (MISO), these "influence" operations are squarely within the scope of MISO.
[71] *Id.* at 44–48.
[72] *Id.*

with traditional military practice.[73] Unfortunately, these elements are broadly defined, and leave significant room for ambiguity and conflicting interpretations.

The traditional "Title 10/Title 50" lexicon is not helpful in resolving the conflicting interpretations.[74] Title 10 of the U.S. Code generally applies to military or Department of Defense authorities,[75] and Title 50 generally establishes authorities within the intelligence community.[76] However, the division between the DOD and the intelligence community is not so clear. Title 10 authorizes certain unacknowledged missions, such as MISO[77] and direct action,[78] by United States Special Operations Command; missions that could otherwise meet the threshold definition of covert actions.[79] Furthermore, Title 50 and Executive Order 12333[80] authorize the Secretary of Defense (SECDEF) to collect and analyze both "defense or defense related" intelligence through clandestine means, as well as to exercise control over those elements of the intelligence community (such as the National Security Agency) which are within the DOD.[81]

Part of the difficulty in applying the current TMA framework is the broad degree of institutional and functional overlap between the Department of Defense and the Intelligence Community.[82] This encompasses both a functional overlap in

---

[73] John Goodin, "Traditional Military Activities" and the Use of Historical Precedent in Covert Action Analysis 10 (2012) (Unpublished primer, The Judge Advocate General's Legal Center and School) (on file with the International and Operational Law Department, The Judge Advocate General's Legal Center and School).

[74] *See, e.g.*, Wall, *supra* note 50, at 49.

[75] *See, e.g.*, 10 U.S.C. §§ 161–168 (2006). These statutes provide for the establishment of geographic and functional combatant commands. These combatant commands are responsible for carrying out military and combat operations within either their functional or geographic area of responsibility, subject to the command authority of the Secretary of Defense.

[76] *See, e.g.*, 50 U.S.C. §§ 3023, 3024 (2004). These sections establish the office, and define the responsibilities of, the Director of National Intelligence. Chapters 45–46 of Title 50 deal with more specific intelligence community roles such as Intelligence Community Authorities, budgeting, and coordination, the role of the Central Intelligence Agency, and the Role of the NSA. 50 U.S.C. Chs. 45–46.

[77] Formerly psychological operations, or PSYOP. National Defense Authorization Act, Fiscal Year 2012 § 1086, PUB. L. 112-81 (2011) [hereinafter NDAA 2012].

[78] "Direct action" is defined as "short-duration strikes and other small-scale offensive actions conducted with specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets in hostile, denied, or diplomatically and/or politically sensitive environments." JOINT CHIEFS OF STAFF, JOINT PUB. 3-0, JOINT OPERATIONS, at GL-17 (17 Sept. 2006, w/ch. 1) [hereinafter JP 3-0].

[79] 10 U.S.C. § 167.

[80] Executive Order 12333 provides executive controls on the intelligence community. It provides guidance for collection of intelligence on "U.S. persons," prohibits practices such as assassination, provides for Congressional oversight of intelligence activities, and identifies the roles, or "lanes" of the various components of the intelligence community. Exec. Order No. 12,333, 3 C.F.R. 200 (1981) [hereinafter E.O. 12,333].

[81] 50 U.S.C. § 3038 (2011) ("Responsibilities of the Secretary of Defense pertaining to the National Intelligence Program"); E.O. 12,333, *supra* note 81.

[82] *See, e.g.*, Interview with Gary C. Schroen by PBS Frontline (Jan. 20, 2006), http://www.pbs.org/wgbh/pages/frontline/darkside/interviews/schroen.html [hereinafter Schroen

conducting operations, as well as an institutional overlap where elements of the national security apparatus are part of both the military and intelligence communities.[83] This phenomenon, termed "convergence," predates the conduct of cyberspace operations by decades.[84] Convergence has caused significant consternation in Congress and the executive branch.[85] The House and Senate Intelligence committees have attempted to subject more unacknowledged military operations to the current reporting requirements of covert action;[86] or more simply have attempted to amend the covert action statute in order to encompass unacknowledged military operations.[87] However, these attempts have failed as the Pentagon opposes such a change,[88] and the Armed Services Committees (HASC and SASC) are apparently satisfied with the level of oversight they exercise over unacknowledged military actions.[89]

The congressional intelligence committees are concerned that the DOD conducts unacknowledged activities under military authorities in order to avoid congressional oversight.[90] Intelligence committee failures to implement more stringent statutory requirements reflect Armed Services Committee oversight of DOD activities. This oversight includes reporting of "Special Access Programs" (SAP), which are classified programs that limit information to certain personnel

---

Interview] (describing the "superb" relationships between CIA and SOF (or "A-Team") operatives, and the "seamless" integration of efforts once the efforts moved beyond the growing pains of initial integration); s*ee also* Emptywheel, *Hiding our Cyberwar from Congress*, SHADOWPROOF (Jan. 14, 2011), https://shadowproof.com/2011/01/14/hiding-our-cyberwar-from-congress/ (including a quote from John Rizzo, former Deputy Counsel for the CIA, in which Mr. Rizzo expresses concern over the ability of DOD to conduct cyberspace operations that look like Title 10 intelligence activities, but with what he perceives as too little oversight by Congress. "…I've always been envious of my colleagues at the Department of Defense because under the rubric of Title 10, this rubric of 'preparing the battlefield.' They have always been able to operate with a—to my mind—a much greater degree of discretion and autonomy than we lawyers at the CIA have been, have had to operate under. . . .").

[83] *See, e.g.*, Ellen Nakashima, *NSA, Cyber Command Leadership Should be Split Up, Officials Advocate*, WASH. POST (Nov. 29, 2013), http://www.washingtonpost.com/world/national-security/nsa-us-cyber-command-leadership-should-be-split-up-officials-advocate-according-to-sources/2013/11/29/09fb5c02-5904-11e3-8304-caf30787c0a9_story.html.

[84] Chesney, *supra* note 57, at 545.

[85] *Id.* at 541; Wall, *supra* note 50, at 102.

[86] H. Permanent Select Comm. on Intelligence, Report to Accompany the Intelligence Authorization Act for Fiscal Year 2010, H. R. Rep. No. 111-2701, at 50 (Jun. 29, 2009). The report articulated concerns over "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." The report went on to label clandestine OPE activities as attempts to circumvent the covert action reporting statute at 50 U.S.C. § 3093.

[87] Bill Gertz, Congress to Restrict Use of Special Ops: Presidential Finding Would be Required, WASH. TIMES, Aug. 13, 2003, at A1.

[88] Jennifer Kibbe, *The Rise of the Shadow Warriors*, FOREIGN AFF. (Mar./Apr. 2004), http://www.foreignaffairs.com/articles/59713/jennifer-d-kibbe/the-rise-of-the-shadow-warriors.

[89] Wall, *supra* note 50, at 104.

[90] H. R. REP. NO. 111-2701, *supra* note 86, at 50; Gertz, *supra* note 88.

regardless of security clearance.[91] This SAP reporting includes a description of the program, funding, and completion milestones.[92] However, the Armed Services Committees are not the only entities to exercise oversight over military activities fitting into the Title 50 intelligence sphere.

There is a degree of shared oversight between the intelligence and the armed services committees where military organizations support Title 50 intelligence community operations.[93] While the covert action statute requires greater specificity than does reporting of military SAPs[94] or support to Title 50 activities,[95] the armed services committees are clearly satisfied with the scope of their oversight and unwilling to adopt more stringent proposals by the intelligence committees, thereby causing tension between these two powerful committees. In some ways the consternation of the intelligence committees, and the intransigence of the armed services committees reflect the "stovepipe" perception that intelligence activities are wholly separate and distinct from military activities.[96] This constitutes a remarkable failure of Congressional understanding in light of convergence since the 1970s,[97] a trend that has only accelerated since the September 11, 2001 terrorist attacks and the resultant global war on terror.[98]

In light of convergence, other executive agencies have concerns that the military is intruding on traditional intelligence community roles such as human

---

[91] 10 U.S.C. § 119 (1987); U.S. DEP'T OF DEF., DIR. 5205.07, SPECIAL ACCESS PROGRAM (SAP) POLICY ¶4, Encl. 4 (July 1, 2010) [hereinafter DODD 5205.07].

[92] Chesney, *supra* note 57, at 613.

[93] Wall, *supra* note 50,251 at 103–04. This shared oversight includes situations in which either the DOD provides support to intelligence community agencies (and vice versa) as well as operations such as the raid to kill Osama bin Laden when the President tasks military assets to conduct covert action (despite CIA Director Panetta's acknowledgment of the operation, and his overall "command" role). *See also* E.O. 12,333, *supra* note 81, ¶ 1.7(a)(4) ("No agency except the [CIA] (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 Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct covert activity unless the President determines that another agency is more likely to achieve a particular objective.").

[94] *See, e.g.*, DODD 5205.07, *supra* note 92. Paragraph 4.f, and Enclosure 4 of DODD 5205.07 require reporting to designated intelligence committee members and their staffs, in addition to members of the armed services committees.

[95] Wall, *supra* note 50, at 104; Chesney, *supra* note 57 at 614–15.

[96] Wall, *supra* note 50, at 121.

[97] Chesney, *supra* note 57, at 545.

[98] *See, e.g.*, Greg Miller & Julie Tate, *CIA Shifts Focus to Killing Targets*, WASH. POST, Nov. 6, 2010, at A1, http://www.washingtonpost.com/world/national-security/cia-shifts-focus-to-killing-targets/2011/08/30/gIQA7MZGvJ_story.html; Schroen Interview, *supra* note 83 (describing the "militarization" of the CIA, which increasingly took on the role of performing lethal operations in support of the Global War on Terror. Gary Schroen also discusses the nascent collaborative efforts between the CIA, U.S. Special Operations Command (SOCOM) and U.S. Central Command (CENTCOM)). *See also* Ann Scott Tyson, *Boots on Ground, Now Also the Eyes*, CHRISTIAN SCI. MONITOR (Mar. 11, 2004), http://www.csmonitor.com/2004/0311/p01s02-usmi.html (describing the increased intelligence collection role of U.S. Special Operations Forces (SOF), as well as expressing concerns that lines between the CIA and DOD were being blurred).

intelligence (HUMINT), and covert information efforts.[99] These concerns have led to significant disagreement as to whether certain unacknowledged activities and operations are the province of the military, or components of the intelligence community.[100] This confusion and disagreement constitutes a critical vulnerability in U.S. military cyberspace and information operations in the face of a Chinese threat with a mature and integrated cyber and information operations doctrine.[101]

B. *Current Traditional Military Activities Framework*

The covert action statute is primarily a means of striking a balance between Presidential authority to conduct foreign affairs and act as the Commander in Chief on the one hand, and Congressional oversight and accountability on the other. In *Youngstown Sheet & Tube Co. v. Sawyer*, Justice Jackson articulated the seminal framework for analysis of executive power vis-à-vis Congressional authority to check that power.[102] Executive power is at its maximum when the President acts pursuant to congressional authorization.[103] However, the President cannot perform, and Congress cannot authorize, any act that violates the constitution.[104] The President acts in a "zone of twilight" when Congress is silent on the matter.[105] Congressional acquiescence to similar action may bolster an argument that the President has this inherent power.[106] The President's power is at its lowest when Congress prohibits the act.[107] The President may only perform such an act if the congressional check is unconstitutional.[108]

The TMA elements are a means by which this separation of powers issue is addressed with respect to unacknowledged military actions. Based on the existence of the TMA exception, the President enjoys far greater latitude in executing unacknowledged actions where they are purely military in nature.[109]

---

[99] *See, e.g.*, 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. 50 (2006) [hereinafter Hayden Nomination]; Mark Mazzetti, Nominee Promises Action as U.S. Intelligence Chief, N.Y. TIMES, (July 21, 2010), http://www.nytimes.com/2010/07/21/us/politics/21intel.html?_r=0.

[100] Wall, *supra* note 50, at 91.

[101] Timothy L. Thomas, *Chinese and American Network Warfare*, 38 JOINT FORCE QUARTERLY 76, 81–83 (2005). Mr. Thomas discusses the similarities, shared weaknesses, and individual weaknesses of U.S. and Chinese doctrine for cyberspace operations. He concludes that INEW, while far from infallible, does present a mature and integrated strategy for combatting a technologically superior foe via cyberspace. *Id.*

[102] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635–37 (1952) (Jackson, J., concurring).

[103] *Id.* at 635.

[104] *Id.* at 636–37.

[105] *Id.* at 637.

[106] *Id.*

[107] *Id.*

[108] *Id.* at 637–38.

[109] 50 U.S.C. § 3093(e).

However, the statutory history is extremely vague, particularly with regard to defining what is meant by ongoing or anticipated hostilities, and what constitutes the geographic bounds of those hostilities.[110] To address these deficiencies, I propose the following. First, I provide a comprehensive analysis of the current TMA elements and the factors that will determine whether those elements are met for a particular action. Second, I offer a series of recommendations that Congress, the Department of Defense and member organizations should implement to eliminate ambiguity as to whether the TMA exception applies.

1. Commanded by a Military Commander

The first element which must be met for an action to qualify as a TMA is that it must be "under the direction or control" of a United States military commander.[111] Such activities can be classified as traditional military activities even where United States sponsorship of the specific activity is not apparent or intended to be acknowledged.[112] While not normally contentious, the institutional overlap and "dual-hatting" of personnel at the National Security Agency and United States Cyber Command (CYBERCOM) have muddied the waters in regard to who commands cyberspace operations.[113]

This convergence is not limited to "dual-hatting" of personnel such as the SECDEF or the Director, NSA/Commander, CYBERCOM. Operators in the CIA and other intelligence organizations often work side by side with military members of Special Operations Command (SOCOM) in other "unconventional warfare" domains.[114] Hence, these operations are frequently conducted without a formal supported/supporting relationship, but rather in a collaborative effort where the concept of "command" may be unclear.[115] This overlap in institutions, personnel, and authorities creates significant confusion as to what it means for a particular operation to be "commanded by a military commander." This confusion engenders congressional and interagency perception that this overlap is part of an effort to shield unacknowledged military activities abroad from congressional oversight.[116]

---

[110] The Area of Ongoing Hostilities (AOH).
[111] S. REP. 102-85 at 44.
[112] *Id.* This is of course the case assuming that the contemplated action meets the other criteria for a TMA outlined below.
[113] *See, e.g.*, Ellen Nakashima, *White House to Preserve Controversial Policy on NSA, Cyber Command Leadership*, WASH. POST (Dec. 13, 2013), http://www.washingtonpost.com/world/national-security/white-house-to-preserve-controversial-policy-on-nsa-cyber-command-leadership/2013/12/13/4bb56a48-6403-11e3-a373-0f9f2d1c2b61_story.html. Ms. Nakashima describes the leadership structure at the NSA (a member of the intelligence community) and CYBERCOM (a military/DOD command), and the fact that the Director, NSA is also the Commander, CYBERCOM. *Id.*
[114] Wall, *supra* note 50, at 115.
[115] Schroen Interview, *supra* note 83.
[116] H. R. REP. NO. 111-2701 at 50; Emptywheel, *supra* note 83.

However, any focus on the status of operators and the intermediate chain of command is inappropriate in determining whether a particular action is either a military or intelligence activity. The correct focus under the current TMA framework must be on the status of the overall commander. The "military" status of the overall commander can be answered by looking into the authorizing chain of command.[117] If there is a formal support relationship,[118] then the inquiry is fairly simple: the status of the supported agency governs the status of the action. However, there is often a lack of a formal support relationship, and Title 10 and Title 50 organizations often act in a more collaborative manner.[119] In these cases, the status of a "commander" is dependent on the status of the end user, and the approval chain for a particular action.[120] The focus is whether "ownership" of the program or action stems from the Director of National Intelligence (DNI) or SECDEF. Thus, if NSA personnel perform actions in support of CYBERCOM pursuant to a tasking from SECDEF, then the operation is "commanded by a military commander," regardless of the intermediate chain of command.

If this "ownership" inquiry yields no clear answer, then there is a fallback inquiry. In recognition of Congress' primary oversight check being the "power of the purse,"[121] the funding and approval source of an action or program should govern the status of the responsible commander as "military" or otherwise.[122] This provides a straightforward tool to determine whether a particular operation is conducted under military, or intelligence community authorities.[123] Thus, an operation which is funded and approved under the authorities and appropriations granted the DNI would not be "commanded by a military commander," regardless of the uniformed status of the operators,[124] or of any intermediate commander.[125] These two simple inquiries into the "ownership" of the particular action or

---

[117] Wall, *supra* note 50, at 102.

[118] For instance, a Central Intelligence Agency asset tasked by a military commander under authorities stemming from SECDEF.

[119] Jeffrey H. Smith, *Keynote Address: Symposium: State Intelligence Gathering and International Law*, 28 MICH. J. INT'L L. 543, 546–47 (2007) (describing the disagreement and confusion in authorities and oversight for "preparation of the battlefield" [IPB] which takes place "in close collaboration with the U.S. intelligence community").

[120] Wall, *supra* note 50, at 101.

[121] BAKER, IN THE COMMON DEFENSE, *supra* note 66, at 102.

[122] Wall, *supra* note 50, at 107–08.

[123] Or in more specific terms, whether the particular operation or program is "owned" by the Secretary of Defense or the Director of National Intelligence. *See, e.g., id.* at 101.

[124] For example, the raid that killed Osama bin Laden could not have been a TMA as CIA Director Leon Panetta exercised overall command of the mission. *See, e.g.*, Interview by Jim Lehrer with Leon Panetta, PBS NEWSHOUR (May 3, 2011), http://www.pbs.org/newshour/bb/terrorism-jan-june11-panetta_05-03/.

[125] *See* 50 U.S.C. § 3301 (2010), which provides that the Director of National Intelligence is responsible for reporting an detailed budget to the congressional intelligence committees, a budget report which includes defense intelligence programs; *see also* 50 U.S.C. §§ 3326–27 (1991, 1993), which provide limits on DOD expenditures in support of other intelligence agency programs, and prohibits transfers of funds between the DOD and CIA without notification to the congressional intelligence committees.

program, and into the funding source of the action, conclusively answer whether an operation is "commanded" by a military commander.

2. Conducted by Military Personnel

There is less debate over the second element, which requires a specific action to be conducted by military personnel. However, this does not mean that this element lacks complications in light of convergence or the growth of the DOD civilian workforce. The legislative history indicates that TMA "encompass[es] almost every use of uniformed military forces, including actions taken in time of declared war or where hostilities with other countries are imminent or ongoing."[126] Congressional concerns over unacknowledged military operations have more to do with operations that are far removed in time or space from ongoing hostilities, than with the status of the operators.[127] Congressional and intelligence community concerns also focus on the performance of functions seen as traditional intelligence activities.[128] Thus, there appears to be little contention over the "military" status of the operators.

This element of the current TMA framework is easily satisfied where the operators are exclusively uniformed military personnel.[129] In the case of DOD contractors or civilians, such as NSA employees, their status as military or intelligence personal is essentially a question of funding. If they are paid with DOD appropriations then they are military personnel, and if paid by intelligence community appropriations, then they are intelligence personnel.[130] This factor is essentially an extension of the previous analysis with regard to the funding stream for the overall action.[131] In this case, the focus is more specific, concentrating on the "funding" of the individual actors, or operators, who carry out a particular mission. The rationale is essentially the same, as this permits oversight by the

---

[126] S. REP. NO. 102-85, at 46. The legislative history indicates that this blanket application to "almost every use of uniformed military forces" includes conventional warfare, contingency operations, hostage rescue operations, "other counterterrorist objectives" such as extraterritorial apprehension, counter-narcotics operations abroad, and other actions to "achieve other limited military objectives." *Id.* Thus, the scope of actions which may be performed by uniformed military personnel under the penumbra of TMA is extensive. The legislative history does indicate that where there is an unacknowledged military operation, which is not part of a larger acknowledged operation, then that discrete action would not fit within the intended scope of TMA. *Id.* Therefore, the scope of TMA is significantly broadened where unacknowledged operations are undertaken in support of a larger, acknowledged operation.

[127] *See, e.g.*, Chesney, *supra* note 52 at 223, 231–32. These types of operations which are either outside of an acknowledged AOH, or which take place far in advance of anticipated hostilities, are the types of actions that pose the greatest diplomatic risk. *Id.*

[128] *See, e.g.*, Smith, *supra* note 120, at 546–47; Emptywheel, *supra* note 83.

[129] S. REP. NO. 102-85, at 46.

[130] *See, e.g.*, 50 U.S.C. § 3607(d) (1992) (prohibiting military personnel conducting overseas operations for the NSA from being paid under both Title 50 and Title 37, entitled Pay and Allowances of the Uniformed Services). Thus, individual operators are paid either under Title 50 or as a member of the uniformed services under Title 37, but not both.

[131] *See* Wall, *supra* note 50, at 107.

Congressional committee that establishes authorizations and appropriations for a particular activity or agency, and the ability to exercise the power of the purse with regard to the particular action or program at issue. Thus, to the extent that NSA personnel, paid by the DOD, perform actions pursuant to a tasking from SECDEF, they would be "military personnel." The same rationale would apply if contractor personnel were performing work under contract paid by the DOD.

This funding analysis to determine an individual operator's status as military is somewhat limited as unconventional lethal operations could certainly involve both military and intelligence community personnel operating side by side overseas.[132] In this context, there are a number of approaches to determine whether a particular operator is military. One such possibility is whether the person would be subject to jurisdiction under Article 2 of the Uniform Code of Military Justice (UCMJ),[133] or whether the person is subject to criminal sanction under the Military Extraterritorial Jurisdiction Act (MEJA).[134] Regardless, the inquiry into the "military" status of operators is greatly streamlined by following one of these simple approaches.

3. Pursuant to Ongoing or Anticipated Hostilities in Which the U.S. Role in the Overall Operation is Apparent or to be Acknowledged

The third element needed for an action to qualify as a TMA is that the action must be pursuant to either ongoing or anticipated hostilities in which the U.S. role in the overall operation is apparent, or to be acknowledged.[135] While this element appears relatively straightforward, its application is more complex.

All stakeholders accept that where hostilities are ongoing and the U.S. role is apparent, then any unacknowledged military actions within an Area of Ongoing

---

[132] *See, e.g.*, Miller & Tate, *supra* note 99 (discussing "omega" or "cross matrix" teams which are composed of combined CIA and military special operations personnel).

[133] 10 U.S.C. § 802 (2013).

[134] 18 U.S.C. § 3261 (2000). It is unclear whether a statute subjecting a person to criminal jurisdiction is a sufficient trigger to unrelated presidential decision-making and congressional oversight rules. However, it is logical that a person meeting two criteria can be effectively in a "military" status: the person (1) performs a U.S. military mission abroad, and (2) is subject to military or criminal jurisdiction due to her status. A non-military member is subject to UCMJ jurisdiction if she is either "serving with, employed by, or accompanying the armed forces," or "within an area leased by or otherwise reserved or acquired for the use of the United States which is under the control of the Secretary [of Defense]" overseas. 10 U.S.C. § 802(a)(10), (12). A non-military member is subject to MEJA jurisdiction if he is "employed by or accompanying the Armed Forces outside the United States." 18 U.S.C. § 3261(a). In either case, regardless of the person's actual uniformed status, if one is both conducting a military mission and subject to criminal jurisdiction due to a statutorily created "military status," then that person's actions can be attributed to the military. Because NSA personnel cannot be paid as both Title 50 personnel and as members of the uniformed services, it is unlikely that an inquiry into their statutory "military status" for criminal jurisdiction purposes is necessary. 50 U.S.C. § 3607(d). *See also* E.O. 12,333, *supra* note 81; Chesney, *supra* note 57, at 607–08.

[135] S. REP. NO. 102-85, at 46.

Hostilities (AOH) are TMA,[136] and there is no need for presidential or SECDEF approval.[137] When there are no ongoing hostilities, then the inquiry turns to "anticipated hostilities." Hostilities are anticipated when the President or SECDEF has approved operational planning for an overall operation.[138] In cases of anticipated hostilities, the TMA exception requires that either the President or SECDEF also approve the specific action.[139] This serves the function of ensuring a degree of executive branch accountability in the case of unacknowledged military actions without ongoing hostilities or apparent U.S. involvement.

a) Overall Hostilities in Which the U.S. Role is Apparent or to be Acknowledged

According to the legislative history, the TMA exception does not apply to the use of military personnel to perform operations that will have a military or political objective abroad, and where there is no intent to acknowledge U.S. involvement.[140] This rule holds regardless of whether or not these operations are "in support" of larger military operations.[141] Thus, any unacknowledged military activities undertaken to influence military or political objectives abroad would necessarily be classified as covert actions, and be subject to the applicable decision-making and oversight schemes. However, actual practice reflects the common-sense approach that unacknowledged individual actions fit within the TMA framework when they are part of a larger overall operation or hostilities in which the U.S. role is apparent or acknowledged.[142] For example, the military conducted extensive MISO operations in Afghanistan during Operation Enduring Freedom.[143] Yet there is no indication that these operations caused concern in Congress, and historical practice indicates that any such unacknowledged activities would have been viewed as TMA to the extent that they took place within the Afghan theater of operations.[144] These actions are in contrast to the case where a separate and discrete unacknowledged action is not part of larger ongoing hostilities, and would not be TMA.[145]

The term "overall operation" applies to the ongoing or anticipated hostilities as a whole, rather than the specific activity being contemplated.[146] Thus, an unacknowledged specific action can qualify as a TMA if it supports

---

[136] *See* Chesney, *supra* note 52, at 225–26.
[137] *Id.* at 224.
[138] S. REP. NO. 102-85, at 46.
[139] *Id.*
[140] *Id.*
[141] *Id.* at 46–47.
[142] *See* Wall, *supra* note 50, at 136.
[143] *See* ARTURO MUNOZ, U.S. MILITARY OPERATIONS IN AFGHANISTAN: EFFECTIVENESS OF PSYCHOLOGICAL OPERATIONS 2001–2010 95–108 (2012) (discussing the various means of dissemination of psychological operations and their prevalence in Operation Enduring Freedom).
[144] *See* Wall, *supra* note 50, at 136; Chesney, *supra* note 57, at 603, 608–09.
[145] S. REP. NO. 102-85, at 46.
[146] *See id.* at 46; Wall, *supra* note 50, at 136.

either ongoing or anticipated operations in which the U.S. role is apparent or intended to be acknowledged.[147] This proposition is uncontroversial, at least in the context of cyberspace operations and other unacknowledged uses of force within Afghanistan and Iraq, where the United States was engaged in overt hostilities.[148] These types of overall operations encompass contingency and counterterrorist objectives, [149] including a myriad of operations such as extraterritorial apprehension, counter-narcotics operations abroad, or other actions to achieve military objectives.[150] This definition of "overall operation" casts a decidedly broad net over the type of overall operation that is considered a military mission in the context of hostilities. The reference to contingency and counterterrorist operations indicates that many overall operations short of combat operations constitute hostilities for TMA purposes. Thus, so long as the overall operation meets this prong, any particular unacknowledged action pursuant to these objectives is a TMA.

The prong requiring that the U.S. role in the overall operation be apparent or acknowledged is met "where the United States *intends* to acknowledge its sponsorship *at the time* the military contingency operation takes place."[151] Thus, the intent to acknowledge must exist at the time the action takes place, but the actual acknowledgement may take place at any point in the future. While independent unacknowledged actions to influence political or military conditions in a foreign country would generally not qualify as TMA in isolation,[152] specific actions qualify as TMA if the U.S. role in the overall operation is either apparent or intended to be acknowledged.[153]

In many ways, the question of whether the U.S. role is apparent is a simple common-sense analysis in the case of ongoing hostilities. First, is there a formal instrument indicating that the U.S. is involved in hostilities? This could include either a declaration of war,[154] or an AUMF[155] indicating that the U.S. is engaged

---

[147] S. REP. 102-85, at 46–47; H. R. REP. NO. 102-166, at 28–30 (1991).
[148] *See, e.g.*, Chesney, *supra* note 52, at 221–22; Eric Schmitt & Mark Mazzetti, *Secret Order Lets U.S. Raid Al Qaeda*, N. Y. TIMES (Nov. 10, 2008), http://www.nytimes.com/2008/11/10/washington/10military.html?pagewanted=2&hp (describing a 2004 order from Secretary Rumsfeld, and explaining that authorities for the use of force by unacknowledged and undisclosed elements of U.S. Special Operations Forces were more permissive in Iraq and Afghanistan where hostilities were ongoing, and less permissive in other nations such as Somalia, Pakistan, and Syria).
[149] S. REP. NO. 102-85, at 46.
[150] *Id.*
[151] *Id.* (emphasis added).
[152] *Id.*
[153] *See, e.g.*, Chesney, *supra* note 57, at 600. Chesney explains that pursuant to ongoing overt hostilities in which the U.S. role is acknowledged, the decision-making rules requiring presidential or SECDEF approval of a specific unacknowledged operation are relaxed. In such cases, unacknowledged operations can be approved by uniformed commanders.
[154] U.S. CONST. art. I, § 8.
[155] *See, e.g.*, Authorization for the Use of Military Force Against Iraq Resolution of 2002, Pub. L. No. 107-243, 116 Stat. 1498.

in ongoing hostilities. Another instrument could be a notification from the President pursuant to the War Powers Resolution.[156] One might also include informal public acknowledgments of the U.S. role or action in a particular operation.[157] This is by no means an exhaustive list, but is meant to provide an indication of the straightforward nature of the inquiry.

If the U.S. role is not apparent, then an action can still qualify as TMA if the U.S. Government intends to acknowledge its role in the overall operation.[158] In this case there is no requirement that an overall operation be acknowledged either at the time it takes place, or at any point in the future; the requirement is satisfied so long as acknowledgment is intended at some point.[159] The inquiry here must focus on whether there is either a temporal or factual set of conditions precedent to the acknowledgement of U.S. participation in the overall operation. The difficulty in determining whether the U.S. government intends to acknowledge an operation is that there is no temporal requirement in either the statute or the legislative history that an operation be acknowledged within a particular amount of time.[160] In this respect, both the intent to acknowledge a particular action or overall operation, as well as the conditions precedent to that acknowledgment ought to be clearly recorded prior to the execution of that action.

There are two further contentious issues raised when discussing actions pursuant to ongoing or anticipated hostilities. The first is when unacknowledged military actions are remote in time, or take place far in advance of ongoing hostilities.[161] The second is raised when unacknowledged operations take place during ongoing hostilities, but are remote in space or geography from the AOH.[162]

b) Remote in Time from Ongoing Hostilities

The Congressional intelligence committees have expressed increasing frustration over unacknowledged military operations taking place far in advance of any anticipated or planned hostilities.[163] Congress particularly laments the use

---

[156] *See, e.g.*, Letter from Barack Obama, President of the United States, to the Speaker of the House of Representatives and the President Pro Tempore of the Senate (Sept. 23, 2014), https://www.whitehouse.gov/the-press-office/2014/09/23/letter-president-war-powers-resolution-regarding-iraq [hereinafter War Powers Resolution Notice of Sept. 23, 2014].

[157] Dan Roberts & Spencer Ackerman, *Barack Obama Authorizes Air Strikes Against ISIS Militants in Syria*, GUARDIAN (London) (Sept. 11, 2014), http://www.theguardian.com/world/2014/sep/10/obama-speech-authorise-air-strikes-against-isis-syria.

[158] *See* 50 U.S.C. § 3093(e).

[159] Wall, *supra* note 50, at 130.

[160] *See* 50 U.S.C. § 3093(e); S. REP. NO. 102-85, at 45–48; H. R. REP. NO. 102-166, at 28–30.

[161] *See, e.g.*, S. REP. NO. 102-85, at 46–47; H. R. REP. NO. 111-186, at 48 (2009); H. R. REP. NO. 102-166, at 28–30; Smith, *supra* note 120, at 546–47.

[162] *See generally* Kenneth Anderson, *Targeted Killing and Drone Warfare: How We Came to Debate Whether There Is a 'Legal Geography of War,' in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW (Peter Berkowitz ed., 2011), http://www.futurechallengesessays.com; Chesney, *supra* note 57 at 603.

[163] *See, e.g.*, H. R. REP. NO. 111-186, at 48; H. R. REP. NO. 102-166, at 28–30.

of the moniker "operational preparation of the environment" (OPE) by the military, and many believe that the label is applied to avoid congressional oversight.[164] Congress's concern is that OPE is often undertaken so far in advance of ongoing hostilities that any connection between the specific action and the overall ongoing hostilities is not apparent to an outside observer.[165]

In this regard, intelligence committees' focus on the temporal aspect is misplaced. First, there is no temporal requirement in order for an action to qualify as pursuant to anticipated hostilities in either the statute or legislative history.[166] This is significant in light of the fact that attempts to impose greater restrictions on the scope of TMA have failed in the face of opposition from both the Pentagon, and within Congress from the armed services committees.[167] Second, to the extent that the intelligence committees are concerned about presidential or executive accountability for diplomatically risky actions,[168] this concern is answered by requiring presidential or SECDEF approval for both the overall operation, and the specific unacknowledged action or program.[169] Intelligence committees' consternation over this aspect of the TMA definition is misplaced in light of the current statute, and appears motivated by a desire to increase their oversight over an area not currently within their sphere of influence.

c) Remote in Space/Geography from an Area of Ongoing Hostilities (AOH)

The second concern arises when there are ongoing hostilities, but an unacknowledged operation is so physically distant from those hostilities that the apparent connection between the two is tenuous. There are significant political and diplomatic risks when U.S. operations impact nations far removed from the AOH.[170] For example, in the aftermath of the U.S. military operation to capture Anas al-Libi,[171] the Libyan government complained that it was not informed

---

[164] Chesney, *supra* note 57, at 604.
[165] H. R. REP. NO. 111-186, at 48; Chesney, *supra* note 57, at 604.
[166] *See* 50 U.S.C. § 3093 (defining covert activities as those activities which are not "intended" to be acknowledged). Furthermore, the legislative history indicates that the "covert action" definition applies to activities in which the U.S. government's role is "not intended to be apparent or acknowledged publicly," and that "concealment or misrepresentation" as to the nature and objectives of U.S. government operations does not render an operation "covert." S. REP. NO. 102-85, at 44–45. In both cases, the focus is on whether the U.S. role is apparent or *intended* to be acknowledged, as opposed to actually being acknowledged.
[167] Kibbe, *supra* note 89.
[168] Chesney, *supra* note 52, at 222–23.
[169] *See* S. REP. NO. 102-85, at 46.
[170] *See* Anderson, *supra* note 163, at 15; Chesney, *supra* note 57, at 610.
[171] Given name: Nazih Abdul-Hamed al-Ruqai. *See* David D. Kirkpatrick, Nicholas Kulish, & Eric Schmitt, *U.S. Raids in Libya and Somalia Strike Terror Targets*, N. Y. TIMES (Oct. 6, 2013), http://www.nytimes.com/2013/10/06/world/africa/Al-Qaeda-Suspect-Wanted-in-US-Said-to-Be-Taken-in-Libya.html?hp (noting Al-Libi was under federal indictment for providing material support to al-Qaeda, specifically "visual and photographic surveillance" of the U.S. Embassy in Nairobi prior to its bombing in 1998).

about the pending operation and termed the capture a "kidnapping."[172] These issues inform an understanding of the diplomatic and political risks that underlie the rationale of the covert action statute, and require a more detailed understanding of the geographic scope of the AOH.

The first instrument that could define the AOH would be an Authorization for the Use of Military Force (AUMF) from Congress. This move falls within the area where a President's power is at its greatest extent according to Justice Jackson,[173] and it stands to reason that congressional oversight in these instances would be much more limited. In this context, where the executive has been granted specific authority to use military force, any unacknowledged military operations within the scope of that AUMF would be at the discretion of the President or his designee(s) within the executive branch. This inquiry is simplified if the AUMF defines geographic bounds for the use of military force, or identifies a specific adversary.[174] Furthermore, if the AUMF references some other document or instrument that identifies an adversary or geographic area, then this informs the geographic bounds of the AOH.[175] The geographic bounds of an AOH need not be limited to any specific country mentioned in the AUMF or other instrument. Though this will provide context on the location of any identified threat; the analysis must be based on the particular circumstances and should consider the threat, the extent to which that threat exists in, or poses a danger to, neighboring states, and other military and diplomatic considerations. Of course, an AUMF may identify a non-state actor or lack geographic limits.[176]

In such cases the executive alone will define the extent of the AOH. While the President may receive less deference from Congress in these matters, the fact remains that the President will still have authority in this "zone of twilight" to define which AOH is appropriate to combat the particular threat.[177] The President enjoys broad power in foreign relations,[178] and absent any Congressional opposition in the form of a joint resolution or other statutory measure the

---

[172] Ernesto Londono & Scott Wilson, *U.S. Strikes al-Shabab in Somalia and Captures Bombing Suspect in Libya*, WASH. POST (Oct. 6, 2013), http://www.washingtonpost.com/world/national-security/us-navy-seals-raid-al-shabab-leaders-somalia-home-in-response-to-nairobi-attack/2013/10/05/78f135dc-2e0c-11e3-8ade-a1f23cda135e_story.html. The United States may not be terribly concerned from a practical perspective about the opinions of the Libyan government; however, that does not mean that the U.S. government should ignore the diplomatic risks that these types of operations pose independent of the relative strength of the aggrieved nation.

[173] Youngstown Sheet & Tube, 343 U.S. at 635.

[174] *See, e.g.*, 116 Stat. at 1498.

[175] *See, e.g.*, Authorization for Use of Military Force Against Iraq Resolution, Pub. 678, Pub. L. 102-1, 105 Stat. 3 (1991). The AUMF references a number a number of United Nations Security Council Resolutions (UNSCRs) with respect to Iraqi non-compliance with weapons program sanctions. *Id.* By incorporating these UNSCRs, the AUMF can be construed as identifying Iraq specifically as the adversary for the purposes of military operations pursuant to the AUMF.

[176] *See, e.g.*, Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

[177] *See* Youngstown Sheet & Tube, 343 U.S. at 637.

[178] United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936).

executive branch enjoys considerable latitude to define the appropriate AOH.[179] The first potential source of a defined AOH is any War Powers notification from the President to Congress. This notice may describe the geographic bounds within which force may be used, as President Obama did in his September 23, 2014 letter notifying Congress of air strikes in Iraq to confront the Islamic State of Iraq and the Levant (ISIL).[180] This letter notified Congress of "a series of discrete military operations in Iraq."[181] While not necessarily delineating the AOH, it informs the scope of the AOH such that nations that are geographically remote from Iraq, or ISIL targets, would be outside of the AOH.

In the circumstance that the War Powers Resolution notification gives no indication of the AOH, then the applicable Operations Order (OPORD) or Execute Order (EXORD) must define the AOH.[182] In cases of anticipated hostilities where operational planning must be approved by the President or SECDEF,[183] then the Operational Plan (OPLAN)[184] will control any conversations about the geographic limits of the AOH. Therefore, the OPLAN must be informed by consultation and guidance from the President or SECDEF. Defining the geographic bounds of the AOH, simplifies the question of whether a particular action is part of an acknowledged overall operation. This brings us to the disputed fourth element.

4. "Traditional"

While the Senate report does not contemplate a requirement that a particular operation have a specific historical precedent to be considered "traditional,"[185] there are those who view historical precedent as a fourth element necessary to qualify as TMA.[186] Not all scholars agree, contending that so long as an action meets the other three objective criteria, then the role of historical precedent is inapplicable.[187] Regardless, the characterization of a particular

---

[179] *See* Youngstown Sheet & Tube, 343 U.S. at 637.
[180] War Powers Resolution Notice of Sept. 23, 2014, *supra* note 157.
[181] *Id.*
[182] *See, e.g.*, JP 3-0, *supra* note 79, at GL-3.5. The Area of Operations is the doctrinal concept of "[a]n operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces." *Id.* at GL-5.
[183] S. Rep. No. 102-85, at 46.
[184] This is the document from which the OPORD developed. JOINT CHIEFS OF STAFF, JOINT PUB. 5-0, JOINT OPERATION PLANNING, at II-24 (2007) [hereinafter JP 5-0].
[185] S. Rep. No. 102-85, at 46.
[186] *See, e.g.*, Wall, *supra* note 50, at 113; *but see* Colonel Richard C. Gross, *Different Worlds: Unacknowledged Special Operations and Covert Action*, at 7–9 (Mar. 30, 2009) (unpublished research paper, U.S. Army War Coll.), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA494716 (discussing TMA and excluding the element requiring a historical precedent).
[187] *See, e.g.*, Aaron P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations*, 111 MICH. L. REV. 423, 444–45 (2012) (arguing that congressional authorization of military operations in cyberspace qualifies them as TMA despite their novelty, provided the operations meet the remaining elements); Chesney, *supra* note 52, at 221.

operation as fitting into a military "lane," or complying with "traditional" military practices would certainly bolster a contention that it is an appropriate military activity and should be considered a TMA. Historical precedent is helpful in identifying appropriately military tasks; however, there are other ways to identify whether an operation is a military task or complies with military practice.

a) The Role of Historical Precedent

Former DNI Admiral Dennis Blair articulated that whether a mission is one traditionally performed by the military is a case-by-case determination.[188] Senate Report No. 102-85 discusses the word "traditional," indicating that as used throughout the bill it means that the action must "hew to the purpose" of the applicable exception to covert activity reporting.[189] The question is what the phrase "hew to the purpose" applies to: does it apply to the use of the word "traditional" only in the exception for "traditional counterintelligence" activities, or every use of the word "traditional" in the statute, including the exception for traditional military activities?

While this "hew to the purpose" language appears in the discussion of the exception applicable to "traditional counterintelligence" activities,[190] the inquiry does not end there. The Senate Report indicates that "[t]he bill uses the word 'traditional' *several* times throughout the new definition."[191] The word "several" is defined by Merriam-Webster as "more than two but not very many," or "more than two but fewer than many."[192] The word "traditional" only appears twice in the exception for intelligence and counterintelligence activities.[193] However, the word "traditional" appears four times in all of the statutory exceptions to the covert action decision-making and reporting regime.[194] Because "several" means "more than two," then it would appear that activities within any exception are "traditional" if they "hew to the [applicable] purpose" of the specific exception.[195]

The Senate Report indicates that the term appears throughout the bill, and not only within the subsection pertaining to intelligence and counterintelligence

---

[188] Questions for the Record for Admiral Dennis Blair Upon Nomination to be Director of National Intelligence Before the S. Select Comm. on Intelligence, 111th Cong. 15 (2009); Dennis C. Blair, Prepared Remarks for the U.S. Senate Committee on Homeland Security and Governmental Affairs Hearing, "Ten Years After 9/11: Is Intelligence Reform Working? Part II," (May 19, 2011).
[189] S. REP. NO. 102-85, at 44.
[190] *Id.*
[191] *Id.* (emphasis added).
[192] "several." MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/several.
[193] 50 U.S.C. § 3093(e)(1).
[194] 50 U.S.C. § 3093(e)(1)–(4)
[195] The four "traditional" activities which are excepted from the covert action reporting statute are: (1) traditional counterintelligence activities, (2) traditional activities to improve or maintain the operational security of U.S. government programs, (3) traditional diplomatic or military activities, and (4) traditional law enforcement activities. *Id.*

activities.[196] This appears to indicate that the "hew to the purpose" language is applicable to every use of the word "traditional," and not only those within the subsection dealing with "traditional intelligence" activities. Thus, with respect to TMA, a specific action qualifies as "traditional" if it "hews to the purpose" of a military mission. This is the case regardless of whether there is a specific historical precedent. However, the question of whether a new or novel operation must comply with "traditional" military practices regarding the Law of Armed Conflict (LOAC) and sovereignty is more complicated.

b) Traditional Military Practice: Compliance with the Law of Armed Conflict and Neutrality

It is DOD policy to apply LOAC in all military operations, including those not rising to the level of an armed conflict.[197] The term "operations" refers to the broad-stroke employment of the military to accomplish given national security goals.[198] Examples of military operations include those undertaken to achieve broad national security goals within a certain area, such as stability operations, noncombatant evacuation operations, or other objectives.[199] However, each operation will be comprised of subordinate missions, tasks, and actions.[200] In this context, the DOD application of LOAC to all military operations encompasses those broad military actions undertaken to achieve national security objectives. The DOD application of LOAC to all operations includes contingency operations short of the armed conflicts to which LOAC applies by law. This practice of applying the rules of LOAC does not encompass specific tasks or missions within the "overall operation" that would not implicate LOAC if they were performed in an armed conflict. Generally speaking, LOAC exists to safeguard those affected by armed conflict from unnecessary suffering and danger.[201] Thus, operations that do not pose a danger of suffering or injury during an armed conflict are generally outside of the restrictions of LOAC. The DOD is further constrained, in that DOD actions must also comply with international law and sovereignty regimes, whereas there is a colorable argument that the "fifth function"[202] authorizes the CIA to violate international law so long as it complies with domestic law.[203]

---

[196] S. REP. NO. 102-85, at 44.
[197] U.S. Dep't of Def., Dir 2311.01E, DOD Law of War Program para. 4.1 (2006) [hereinafter DOD Dir. 2311.01E].
[198] *See* JP 3-0, *supra* note 79, at I-14.
[199] *Id.* at I-15.
[200] *Id.* at V-3.
[201] *See, e.g.*, Int'l & Operational L. Dep't., Operational Law Handbook 11 (2014).
[202] Chesney, *supra*, note 57, at 586–87. The "fifth function" tasks the CIA "to perform such other functions and duties as the National Security Council may from time to time direct." National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495, §102(d).
[203] U.N. Charter, art. 2, para. 4. *See also* A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 597, 601 (2007).

C. *Military Information Support Operations (MISO)*

Military Information Support Operations (MISO) are "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives."[204] The military conducts MISO under a number of statutory authorities. Special Operations Command (SOCOM) was established by 10 U.S.C. § 167; and the statutory mission of SOCOM includes the authority to conduct MISO.[205] Other statutory authorities place constraints on the conduct of information operations by the military.[206] MISO products may be distributed within the U.S., but MISO will never be targeted to influence public opinion within the U.S, nor will MISO be targeted against U.S. persons outside of the United States; rather, MISO products may only be made available within the U.S. upon request for academic research, journalism, or other purposes that do not seek to influence domestic public opinion or political processes.[207]

The military has also developed doctrine for the employment of MISO.[208] When developing MISO products, originators conduct a detailed Target Audience Analysis (TAA), which informs the remainder of the process,[209] including:[210] (1) Series Development, (2) Product Development and Design, (3) Approval, (4) Production, Distribution, and Dissemination, and (5) Evaluation.

The goal of the TAA is to ensure that MISO messages are designed in a manner, and disseminated by means, most likely to achieve the desired effects on the target audience.[211] Part of the TAA focuses on whether the target audience will be receptive to messages attributed to the U.S.[212] Military Information

---

[204] Joint Chiefs of Staff, Joint Pub. 3-13.2, Military Information Support Operations, at I-1 (2010) [hereinafter JP 3-13.2].

[205] 10 U.S.C. § 167 (2012); 10 U.S.C. § 2011 (2012). These operations, formerly referred to as Psychological Operations (PSYOP), were renamed Military Information Support Operations in 2012. § 1086, 125 Stat. at 1309. For the sake of consistency, this paper will refer to these operations as MISO, regardless of their moniker in the source material.

[206] *See, e.g.*, National Defense Authorization Act, Fiscal Year 2013 § 1078, 22 U.S.C. § 1461 (2012); 10 U.S.C. § 2241a.

[207] JP 3-13.2, *supra* note 205,207 at I-3. Despite concerns that the National Defense Authorization Act, Fiscal Year 2013 authorizes the use of "propaganda" by the U.S. government within the United States, s*ee, e.g.*, Michael Hastings, *Congressmen Seek to Lift Propaganda Ban*, BUZZFEEDNEWS (2012), http://www.buzzfeed.com/mhastings/congressmen-seek-to-lift-propagan da-ban, these messages will not be distributed domestically to influence public opinion. 10 U.S.C. § 2241a; 22 U.S.C. § 1461(c). Other purposes, such as academic research and archiving PSYOP/MISO products, are allowed.

[208] *See generally* JP 3-13.2, *supra* note 205.

[209] *Id.* at V-3.

[210] *Id.* at xiv.

[211] *Id.* at V-43–45.

[212] *Id.* at V-2–3.

Support Operations employ three types of attribution and content.[213] It is the attribution, or U.S. acknowledgement, that potentially renders an activity covert; questions of content are irrelevant. The first type of attribution is "white," which are openly attributed to the U.S.[214] There are also "black" products, under which the attribution is affirmatively false; for example, where U.S. products are attributed to some non-U.S. government entity.[215] Finally, there are "gray" products, which are not attributed to the U.S. government, or any other entity.[216] Because the U.S. government acknowledges "white" MISO products, the covert action definition does not apply.[217] "Black" MISO meet the threshold definition of "covert activities," as the U.S. role would not be apparent nor intended to be acknowledged.[218] "Gray" MISO may also be "covert activities," so long as U.S. acknowledgment is not intended.[219] Once attribution is determined, then the means of dissemination can be addressed.

Traditionally, both MISO and cyberspace operations have been treated as a subset of information operations (IO).[220] However, the proliferation of information technology and network access[221] has contributed to the classification of cyberspace as a distinct operational domain.[222] This being the case, the RAND Corporation advocated separating the content and technical aspects of IO doctrine.[223] The RAND Corporation recommended separating personnel and capabilities responsible for IO into two groups. First are "inform and influence operations" which focus on the content of information operations.[224] The second discipline is "information technical operations" which focus on the means of dissemination.[225] This second discipline would involve the integration of cyberspace operations,[226] electronic warfare, and other electromagnetic media (e.g., radio and television) to disseminate content.[227] The Department of Defense has shifted toward this approach by characterizing cyberspace as a tool to

---

[213] Isaac R. Porche III et al., Redefining Information Warfare Boundaries for an Army in a Wireless World 62 (2013).
[214] *Id.* (citing U.S. Dep't of Army, Field Manual 3-13, Information Operations at 11–1 (2003) [hereinafter FM 3-13]).
[215] *Id.*
[216] *Id.*
[217] *See id.*
[218] *See id.*
[219] *See id.*
[220] *See* FM 3-13, *supra* note 215, at v–vi.
[221] PORCHE ET AL, *supra* note 214, at 7–8.
[222] *See, e.g., id.* at 7; Joint Chiefs of Staff, Joint Pub. 3-12(R), Cyberspace Operations I-2 (2013) [hereinafter JP 3-12(R)].
[223] Porche et al, *supra* note 214, at 41–42, 65.
[224] *Id.*
[225] *Id.* at 42, 65.
[226] *See* JP 3-12(R), *supra* note 223, at II-4–II-12. Cyberspace operations (CNO) include cyberspace defense; cyberspace intelligence, surveillance, and reconnaissance (ISR); cyberspace OPE; and cyberspace attack. These can be pursuant to ongoing hostilities, or in the case of cyberspace OPE, pursuant to anticipated hostilities.
[227] Porche et al, *supra* note 214, at 46–47, 68–69.

disseminate information products.[228] The next section discusses cyberspace operations, and is followed by a discussion of the challenges they pose for the application of the covert action and TMA definitions.

D. *Cyberspace Operations*

Congress has provided statutory authority to DOD to conduct offensive cyber operations.[229] DOD is authorized to carry out offensive cyberspace operations in defense of the United States, its allies, and interests.[230] These operations are subject to two restrictions: (1) offensive cyberspace operations shall be subject to DOD policies and principles for "kinetic"[231] operations including the Law of Armed Conflict,[232] and (2) they will be subject to the War Powers Resolution.[233] The War Powers Resolution governs the introduction of U.S. forces into hostilities, a qualification that does not apply to MISO because pure information operations do not involve any "introduction of forces."[234] Even if cyberspace operations could rise to the level of implicating the War Powers Resolution, MISO would not rise to the level of a "use of force" sufficient to trigger this requirement, as they are information-based and have no physical effects.[235]

In addition to congressional authorization, President Obama has directed DOD to develop and maintain the ability to operate in the cyber domain.[236] The military has adopted a strategic plan for maintaining U.S. preeminence in the

---

[228] *See* JP 3-12(R), *supra* note 223, at I-5–6. While cyber tools are also viewed as a means to achieve effects directly, the Joint Doctrine for cyberspace operations also recognizes that cyberspace can be used as a vehicle to support information operations such as MISO and Military Deception (MILDEC).

[229] § 954, 125 Stat. at 1307. Cyberspace operations include both offensive and defensive operations. Offensive cyberspace operations are "intended to project power by the application of force in and through cyberspace. OCO [Offensive cyberspace operations] will be authorized like offensive operations in the physical domains, via an execute order (EXORD). OCO requires deconfliction in accordance with (IAW) current policies." JP 3-12(R), *supra* note 223 at II-2. A subset of OCO include cyberspace attack operations that seek either to deny or manipulate an adversary's access to information or information systems. *Id.* at II-5.

[230] § 954, 125 Stat. at 1307.

[231] Congress appears to have used the term "kinetic," as a synonym for the accepted military term "lethal." Thus, "kinetic" operations for the purpose of the statute are treated as those which seek to have, or may have, "lethal" effects on a target. *See, e.g.*, JP 3-0, *supra* note 79 at II-11. JP 3-0 differentiates between lethal and nonlethal effects on a target. It does not use the term "kinetic" at all.

[232] The question of whether cyberspace MISO operations are subject to the law of armed conflict was addressed during the discussion of what it means for an activity to be "traditional."

[233] § 954, 125 Stat. at 1307.

[234] War Powers Resolution, 50 U.S.C. § 1541 (1973); *see also* Allison Arnold, *Cyber Hostilities and the War Powers Resolution*, 217 MIL. L. REV. 174, 176–78 (2013).

[235] *See* Arnold, *supra* note 235, at 176.

[236] *See, e.g.*, Nat'l Sec. Strategy of the United States (2010) [hereinafter 2010 Nat'l Sec. Strategy].

cyber domain,[237] and developed a joint doctrine governing offensive, defensive, and intelligence cyberspace operations.[238] U.S. military doctrine divides cyberspace into three layers: the physical, logical, and cyber-persona.[239] The physical layer is composed of the infrastructure: the wires, systems, and hardware that make up the infrastructure of the internet.[240] The logical layer is the foundational language and programming which provides functionality, enabling the end user to interface with the machine.[241] Finally, the cyber-persona, or end user, is the data consumer or producer.[242] The cyber-persona can either take action, or be influenced by operations, in cyberspace.

Cyberspace operations may have impacts in all three layers.[243] However, MISO by their nature can have effects limited to the cyber-persona and logical layers.[244] Military Information Support Operations do not involve physical effects or damage to adversary cyberspace operations infrastructure. Military Information Support Operations can have effects on the cyber-persona when used to disseminate a message aimed at influencing the cyber-persona's actions. Military Information Support Operations can also have effects on the logical layer when used to manipulate the underlying code or logical language to disrupt or alter adversary access to unfriendly messaging. Neither of these involves an impact on the physical infrastructure of the network such as destruction, or otherwise rendering physical objects inoperable. Military Information Support Operations are focused on the cyber-persona in seeking to influence actions by a particular target audience.[245] United States military doctrine treats cyber capabilities as a medium to conduct MISO.[246] Cyberspace operations are used to support IO

---

[237] U.S. Dep't of Def. Cyberspace Pol'y Rep., A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, SECTION 934 1–2 (2011) [hereinafter Cyberspace Pol'y Rep.].
[238] *See generally* JP 3-12(R), *supra* note 223.
[239] *Id.* at I-2.
[240] *Id.* at I-3.
[241] *Id.*
[242] *Id.*
[243] *See id.* at II-6.
[244] For instance, manipulation of the foundational code to control which content a particular user, or users, has access to, or to manipulate user access that would otherwise be available. These are generally captured in the "Deny" and "Manipulate" variations of "Cyberspace Attack." *Id.* at II-5.
[245] *See, e.g.*, JP 3-13.2, *supra* note 205, at IV-3I. This does not rule out the possibility that effects on the cyber-persona could be achieved by manipulating, or otherwise affecting the logical layer in a manner that denies or manipulates the information a cyber-persona may access. *See* JP 3-12(R), *supra* note 223, at II-5.
[246] JP 3-12(R), *supra* note 223, at I-5. This contrasts with the Chinese approach under INEW, which focuses on INEW as an integrated, strategic method to waging warfare (one which is essentially inseparable from information operations and "kinetic" military operations). The U.S. views cyber capabilities as more akin to tools that provide a technological edge. This aligns with the Chinese belief that INEW is a necessary strategy and means to combat a technologically superior foe, and not simply "one more tool in the toolkit." *See, e.g.*, Thomas, *supra* note 102, at 82.

objectives, and are integrated with other types of operations.[247] Thus, DOD has adopted the use of cyberspace as a medium to reach the cyber-persona.[248]

E. *Complications of TMA in the Cyber Context: Convergence and the Physical Layer*

The emergence of the U.S. ability to conduct unacknowledged MISO in cyberspace poses particular complications in application of the current TMA framework. Some of these complications, such as questions of sovereignty, arise because of the nature of operations in cyberspace. Other complications arise because of the structure and doctrine concerning U.S. cyberspace and information operations. These concerns include the unique structure of the NSA within the DOD, and the fact that the Director, NSA is also the Commander, CYBERCOM. Other doctrinal concerns include the use of MISO and cyberspace operations to conduct OPE significantly in advance of any ongoing hostilities. Each of these complications bears upon the four elements of the TMA framework identified in Section B.

1. Commanded by a Military Commander, and Conducted by Military Personnel

There is significant institutional overlap of personnel and infrastructure between the National Security Agency (NSA) and U.S. CYBERCOM.[249] This convergence is further complicated by the structure of the U.S. intelligence community,[250] because the NSA is part of the intelligence community but also part of the Department of Defense.[251] Furthermore, the Secretary of Defense has intelligence responsibilities, which he exercises through the NSA as well as other DOD components of the intelligence community.[252] This framework complicates the determination of whether a specific action is a military or intelligence action. This is exacerbated as the Commander, CYBERCOM[253] is the same person as the

---

[247] JP 3-12(R), *supra* note 223, at I-5.
[248] *Id.* at I-4; PORCHE ET AL, *supra* note 214, at 42.
[249] Chesney, *supra* note 57, at 581.
[250] The term "intelligence community" comprises specified agencies and activities within the U.S. government that have designated national intelligence responsibilities. The term was established, and member agencies identified in E.O. 12,333, *supra* note 81. In particular, paragraphs 1.3 and 1.4 establish the term "intelligence community" and identify member agencies. A current listing of the member agencies of the U.S. intelligence community can be found on the website of the Office of the Director of National Intelligence, http://www.dni.gov/index.php/intelligence-community/members-of-the-ic.
[251] Wall, *supra* note 50, at 116–17.
[252] E.O. 12,333, *supra* note 81. Part 1.10 delineates the Secretary of Defense's intelligence responsibilities as including both national and military intelligence, and Part 1.7 identifies components of the intelligence community that the *Secretary* of Defense may use.
[253] The Commander, CYBERCOM is a military commander, who reports to SECDEF. *U.S. Cyber Command*, UNITED STATES STRATEGIC COMMAND, https://www.stratcom.mil/factsheets/2/Cyber_Command/.

Director, NSA.[254] This structural organization poses further complications as personnel conducting cyberspace operations at the NSA may be uniformed military personnel operating under intelligence authorities, or may be DOD civilians operating under military authorities. In many ways, these structural questions are the simplest to answer, either through clarifying authorities or modifying structures. In contrast, the nature of cyberspace operations creates more complex questions.

2. Pursuant to Ongoing or Anticipated Hostilities in Which the U.S. Role in the Overall Operation is Apparent or to be Acknowledged

Cyberspace as a domain affords near unprecedented operational reach, and an ability to conduct operations at previously unimagined speeds. These characteristics allow the use of cyberspace tools to conduct operations significantly in advance of ongoing hostilities. Capabilities in cyberspace provide the U.S. military the opportunity to conduct unacknowledged information and non-lethal operations to prepare the battlespace for follow on operations. In such cases, either the President or SECDEF must approve both operational planning for the follow on operation, as well as the specific activity in question.[255] Congress has expressed concern that this trigger provides insufficient presidential accountability and insufficient risk management for "Operational Preparation of the Environment" (OPE) far in advance of ongoing hostilities.[256] Military Information Support and cyberspace operations are no different in this respect. Cyberspace operations are a means for the U.S. military to conduct OPE.[257] Cyberspace OPE includes operations to plan and set conditions for subsequent military operations, including gaining access to adversary systems.[258] Additionally, MISO may be conducted in either peacetime or in support of combat operations,[259] and are undertaken to shape the environment and deter aggression before the advent of hostilities.[260] Therefore, both MISO and cyber operations could be classified as "covert operations" performed to influence conditions abroad.[261]

United States military doctrine specifically contemplates the use of cyber capabilities to conduct OPE.[262] With cyber capabilities as the means to disseminate,[263] MISO are also employed to set conditions for military success

---

[254] The Director, NSA is the head of an intelligence community component that reports to the Director of National Intelligence. *Organization*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, http://www.dni.gov/index.php/about/organization.
[255] S. Rep. 102-85 at 46.
[256] Goodin, "Traditional Military Activities" (unpublished primer), *supra* note 74 at 8.
[257] JP 3-12(R), *supra* note 223 at II-2.
[258] *Id.* at II-5.
[259] JP 3-13.2, *supra* note 205 at I-5.
[260] *Id.*
[261] 50 U.S.C. § 3093.
[262] JP 3-12(R), *supra* note 223 at II-5.
[263] *Id.*

prior to overt hostilities.[264] Therefore, MISO would be employed via cyber channels in advance of anticipated hostilities. Indeed, the possibility exists that the military could conduct unacknowledged cyberspace operations when no ongoing hostilities ever take place, so long as either the President or SECDEF has authorized operational planning and the specific action.[265]

In addition to these temporal concerns, cyberspace operations also pose concerns related to the "location" of an operation in relation to an AOH. The ability to reach adversaries such as non-state actors will often—if not always—require network intrusion and effects in neutral nations.[266] The three layers of the cyber domain do not necessarily coincide with national boundaries.[267] Thus, a cyberspace MISO that is targeted to influence a cyber-persona within an AOH may involve data traffic, intrusions, or logical effects on the physical layer located outside of the AOH.[268] The question then, is whether a cyberspace operation "takes place" within a targeted nation, or within other nations through which the data traffic passes. Other questions about state sovereignty in cyberspace, as well what type of cyberspace operations would violate the sovereignty of a neutral nation, will be addressed in Subsection 3.b of this Section.[269]

Because of the structure of the physical layer of cyberspace,[270] cyberspace operations will often involve data transmission through neutral nations far removed from the AOH.[271] This is problematic because of the unsettled state of international law with respect to sovereignty in cyberspace.[272] Due to the fragmented nature of data transmission in cyberspace, mere data transmissions will almost never have effects on neutral nations, or outside of the nation targeted in a cyberspace operation.[273] Military Information Support Operations add a particular set of concerns. On one hand, the information disseminated may be accessible to audiences far removed from an AOH. At the same time, the

---

[264] JP 3-13.2, *supra* note 205 at I-6.
[265] S. REP. 102-85 at 46.
[266] Ellen Nakashima, *Pentagon is Debating Cyber-Attacks*, WASH. POST (Nov. 6, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507464.html; Chesney, *supra* note 52 at 231–32.
[267] JP 3-12(R), *supra* note 223 at I-2.
[268] *See, e.g.*, Ellen Nakashima, Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield, WASH. POST (Nov. 6, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html.
[269] *See generally* Lt. Col. Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 A.F. L. REV. 1 (2009).
[270] JP 3-12(R), *supra* note 223 at I-2.
[271] Nakashima, *supra*, note 267; Chesney, *supra* note 52 at 221.
[272] Franzese, Sovereignty in Cyberspace, *supra* note 270.
[273] Memorandum from the Network Working Group, Cisco Systems 15, ¶ 2.1, 97, ¶ 5.3.9 (F. Baker, ed., June 1995), http://tools.ietf.org/html/rfc1812. This memorandum describes the basic infrastructure of the internet, including the method of data transmission. Specifically, data is broken into packets of manageable size, and the entire combination of data packets is then reassembled upon reaching its destination. Thus, code used to carry out a cyberspace operation will not be fully compiled except at the point of origin and at the target.

information is—and doctrinally should be—calculated and employed to have an effect only on a specific target audience.[274]

To the extent that the presidential decision-making and congressional oversight rules are about managing diplomatic risk;[275] it makes sense to conclude that operations that take place within a defined AOH are "pursuant" to those ongoing hostilities. There are two questions presented by this focus on the geographic bounds of the AOH. First, with respect to a cyberspace MISO operation, where does the operation "take place?" The second question is how to define that AOH.[276] Both questions are exacerbated in the cyber context where such actions can involve network intrusions in neutral countries far removed from the AOH.[277]

Discussion of where a MISO operation "takes place" begins with the concept of Target Audience Analysis. TAA is conducted to tailor the message, content, and delivery means of MISO products to maximize the effects on the target audience.[278] It stands to reason that a MISO designed to have effects on one particular targeted audience, should have limited impact on non-target audiences. Furthermore, U.S. cyber doctrine relies on the ability to focus effects on a specific cyber-persona, or target set.[279] Because cyberspace operations are fragmented until reaching their intended target, it follows that cyberspace MISO should only have observable effects at the cyber-persona level of a desired target audience. Therefore, the inquiry into where a particular cyber MISO operation "takes place" must focus on the physical location of the targeted cyber-persona, or audience. Once the location of the target audience of a MISO is identified, and the cyber tools are effectively tailored to target the effects, then the question becomes whether that audience or cyber-persona is within the AOH as discussed previously.

3. Traditional Military Practice

The question of traditional military operations, or historical military practice also poses complications when taking into account the lack of historical precedent for military operations in cyberspace.[280] However, when cyberspace is viewed as a tool for the conduct of information operations, then the question of whether an operation is "traditional" is simplified.[281] The U.S. military conducted information operations, including PSYOP/MISO in foreign nations during World

---

[274] JP 3-13.2, *supra* note 205 at V-4-5; JP 3-12(R), *supra* note 223 at IV-3 (supporting the proposition that U.S. cyberspace operations capabilities enable targeting a specific cyber-persona).
[275] Chesney, *supra* note 57 at 543.
[276] Anderson, *supra* note 163 at 2–3.
[277] Nakashima, *supra* note 267.
[278] JP 3-13.2, *supra* note 205 at V-3.
[279] JP 3-12(R), *supra* note 223 at II-5.
[280] Brecher, *supra* note 188 at 444–45.
[281] JP 3-12(R), *supra* note 223 at I-6.

Wars I and II.[282] The military retained the authority to conduct MISO as a special operations capability after WWII, even though the Office of Special Services had transitioned to the civilian-controlled Central Intelligence Agency.[283] The MISO and offensive cyberspace missions are also both statutorily authorized to the DOD by Congress.[284] It strains logic to believe that Congress can provide the TMA exception to the covert action statute, grant statutory authority for the military to carry out particular missions, and then claim that some of those very missions are subject to the covert action rules notwithstanding the exception. Because Congress and the President have specifically tasked the military with conducting both MISO and offensive cyberspace operations, these operations "hew to the purpose" of a military mission, and historical comparisons are inapplicable.[285] Furthermore, while it is DOD policy to apply LOAC to all military "operations," [286] this will not necessarily always apply to every MISO or cyberspace operation where there is no LOAC rule governing the particular action.

a) Traditional Military Practice: Compliance with the Law of Armed Conflict

Both MISO and cyberspace operations are subordinate tasks or actions used to support the national security objective which is the goal of the overall "operation."[287] Thus, it is not necessarily true that LOAC is applicable to all types of information or cyberspace operations, even if they were to take place during an armed conflict. Effects achieved via cyberspace in connection with an armed conflict are subject to the restrictions of LOAC.[288] Furthermore, senior officials who order or command cyberspace operations that do violate LOAC bear criminal

---

[282] U.S. Dep't of Army, Field Manual 3-05.30, Psychological Operations at 1–7, 6–14 (Apr. 2005) [hereinafter FM 3-05.30].

[283] *See, e.g.*, Pub. L. No. 99-500 § 9115, 100 Stat. 1783 (1986). This section amended the National Defense Appropriations Act for Fiscal Year 1986, enacted 10 U.S.C. § 167, established Psychological Operations (since re-designated MISO) as a statutory mission, and the capability of U.S. Special Operations Command, prior to the 1991 passage of the covert action statute. *See also*, FM 3-05.30, *supra*, note 283 at 6–16 (describing the conduct of military PSYOPs, with Presidential oversight, during the early years of the Vietnam War).

[284] *See* 10 USC § 167(j)(6); 10 USC § 2011(d)(1) (covering MISO missions). *See also* NDAA 2012, *supra* note 78 at § 954 (covering offensive cyberspace operations).

[285] S. REP. 102-85 at 44–45.

[286] DOD DIR. 2311.01E, *supra* note 199 at para. 4.1.

[287] JP 3-13.2, *supra* note 205 at IV-9; JP 3-12(R), *supra* note 223 at III-1. The use of the term "operations" in both MISO and cyberspace operations appears to be inartful drafting, as these are both tools which can be used in support of a larger operation to achieve national security objectives.

[288] NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE R. 20, at 75 (Cambridge Univ. Press, 2013) [hereinafter TALLINN MANUAL], http://issuu.com/nato_ccd_coe/docs/tallinnmanual. The Tallinn Manual was an effort by a group of international legal scholars, sponsored by the NATO Cooperative Cyber Defence Centre of Excellence, to define international legal norms and obligations with respect to cyberspace operations. *See id.* at 1–11.

responsibility.[289] However, the restrictions of LOAC do not capture all cyberspace operations, and draw a distinction based on effects. Cyberspace operations employed during an armed conflict which are "reasonably expected to cause injury or death to persons or damage or destruction to objects" would be subject to the restrictions of LOAC.[290] However, leaving aside questions of sovereignty and neutrality, other cyberspace operations employed during an armed conflict that do not have physical or lethal effects do not necessarily violate LOAC.[291]

Therefore, while offensive, or effects based, cyberspace operations shall be subject to DOD policies and principles for "kinetic" operations (including LOAC),[292] this qualifying principle is generally inapplicable to cyberspace MISO, as there is no LOAC prohibition on MISO, or information operations generally.[293] Military information support operations are not "kinetic," [294] and are thus generally outside the scope of LOAC.

b) Traditional Military Practice: Sovereignty and Neutrality

Integral to this discussion of the military's traditional adherence to LOAC and international law are questions of sovereignty of neutral states in cyberspace. If sovereignty does exist in cyberspace, what level of intrusion into cyberspace

---

[289] *Id.* R. 24, at 91; Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 49 (Aug. 12, 1949), 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, art. 50 (Aug. 12, 1949), 6 U.S.T. 3217, 75 U.N.T.S. 31 [hereinafter GC II]; Geneva Convention Relative to the Treatment of Prisoners of War, art. 129 (Aug. 12, 1949), 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Geneva Convention Relative to the Treatment of Civilian Persons in Time of War, art. 146 (Aug. 12, 1949), 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV].

[290] TALLINN MANUAL, *supra* note 289, R. 20, 30, 31, 32, at 75, 106–113, ch. 5 at 203 (regarding certain classes of protected persons, objects, and activities such as medical, and religious personnel/facilities).

[291] *See id.* at 192, for the proposition that "cyber espionage" does not violate the law of armed conflict, even though a member of the armed forces committing "cyber espionage" within the territory of a target country does not have combatant immunity for those actions. This is based on customary international law, as reflected in Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulation Concerning the Laws and Customs of War on Land, art. 29–31 (Oct. 18, 1907), 36 Stat. 2277 [hereinafter Hague (IV)], and Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), art. 46 (Jan. 23, 1979), 1125 U.N.T.S. 3 [hereinafter AP I].

[292] NDAA 2012, *supra* note 78 at § 954.

[293] There could be exceptions such as MISO operations that publish photographs of detainees, which could be viewed as an "outrage on personal dignity" in violation of Common Article 3 of the Geneva Conventions of 1949, or making the detainee a "public curiosity" in violation of GC III, article 13. GC III, *supra* note 290 at art. 13. However, these types of LOAC violations are based upon the content of any disseminated MISO message, and not applicable to all classes of MISO messages or missions as a whole.

[294] It is DOD policy that publishing photographs of Enemy Prisoners of War is a violation of the Law of War. *See, e.g.*, JP 3-13.2, *supra* note 205 at I-3. Thus, MISO products which would publish such photos would be subject to the restrictions of LOAC.

justifies a particular response by an affected nation?[295] While radio and wire traffic through neutral nation facilities does not void that nation's neutrality during a conflict,[296] it is unclear whether nonconsensual data or network traffic through servers in a neutral nation violates that nation's sovereignty.[297]

There are scholars who recognize the existence of sovereignty in cyberspace.[298] However, there has been little progress in the way of identifying what types of actions in cyberspace violate state sovereignty.[299] This is critical in the context of cyberspace operations, as current U.S. cyberspace operations aimed at countering internet use by non-state actors will often impact, or pass through physical network infrastructure in neutral nations.[300] Article 2(4) of the United Nations Charter prohibits the "threat or use of force against the territorial integrity or political independence of any state."[301] However, it is unsettled when, and if cyberspace operations can rise to this level.[302]

There are a number of tests articulated for when an action in cyberspace can constitute a violation of sovereignty as a use of force such that force in self-defense is justified. An "instrument based" approach looks at the nature of the "weapon" employed and whether the weapon or attack has physical characteristics "traditionally associated with military coercion."[303] The "target based" approach focuses on the nature of the object attacked and applies a strict

---

[295] *See, e.g.*, Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825 (2012) (addressing the concept of self-defense in response to a cyber "attack" in the context of non-state actors); Reese Nguyen, *Navigating Jus ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1084 (Aug. 2013) (discussing various tests proposed by scholars for determining whether a cyber intrusion merits the resort to force in self-defense).

[296] Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, art. 8-9, Oct. 18, 1907, 38 Stat. 2310 [hereinafter Hague (V)].

[297] Nakashima, *supra* note 269 (indicating that the Department of Justice has issued a draft opinion that such data traffic through neutral nation servers violate that nation's sovereignty unless that nation consents). Such actions would not appear to violate sovereignty, based on application of the neutrality regime regarding wire transmissions through neutral nations established by Hague (V), *supra* note 297 at art. 8–9.

[298] *See, e.g.*, Franzese, *supra* note 270 at 39–40.

[299] For instance, whether sovereignty is implicated when actions in cyberspace affect the physical, logical or cyber-persona level; or whether sovereignty is implicated when actions in cyberspace involve mere traffic trough a system, but have no effect.

[300] *See, e.g.*, Ellen Nakashima, *Cyber-Intruder Sparks Response, Debate*, WASH. POST (Dec. 8, 2011), http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

[301] U.N. Charter art. 2, para. 4.

[302] See generally, CDR Todd C. Huntley, Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare, 60 NAVAL L. REV. 1 (2010).

[303] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041 (2007).

liability standard if the target is of sufficient consequence.[304] Lastly is the "effects based" test, which focuses on the effects caused by a cyber attack on the victim state, and whether those effects are of sufficient consequence to warrant an armed response.[305] In all cases, the location of any effects, determine a nation's interest in self-defense.

Whether an armed response is justified is a different inquiry than whether a state's sovereignty has been violated. However, a strict liability approach that considers any data traffic or network intrusion to be a violation of state sovereignty appears unworkable based on the reality of the physical structure of the internet,[306] and overly strict in light of existing sovereignty and neutrality regimes governing radio and wire transmissions through neutral countries.[307]

Neutral nations have the affirmative obligation to prevent belligerent parties from using their physical territory to move troops and materiel, or to erect dedicated communications facilities for the use of the belligerent party within neutral state territory.[308] However, a neutral nation does not sacrifice its neutrality by allowing belligerent parties to send transmissions using its wire and radio capabilities.[309] This being the case, a strict liability approach to violations of sovereignty is inconsistent with existing international treaty law. Several experts, working on behalf of NATO, have extended the Hague (V) analysis regarding wire and radio transmissions to the physical layer of cyberspace.[310] Thus, instead of a strict liability regime akin to aerial overflight or territorial seas which involve a physical intrusion, international legal scholars have likened cyberspace to other regimes which involve electronic or electromagnetic traffic through the physical layer in neutral states.[311]

---

[304] David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. AND POL'Y 87, 91 (2010).

[305] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914–15 (1999). This "effects based" test has been adopted by the United States. *See* Harold Koh, Legal Advisor, U.S. Dep't of St., Remarks at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm [hereinafter Koh Speech].

[306] Nakashima, *supra* note 269.

[307] Hague (V), *supra* note 297 at art. 8–9 (indicating that a neutral country does not sacrifice its neutral status by allowing use of radio/wire communication facilities to allow transmission by belligerents, so long as that neutral nation doesn't discriminate between/among belligerent states).

[308] *Id.* at art. 5.

[309] *Id.* at art. 9.

[310] TALLINN MANUAL, *supra* note 289 R. 91–95, at 250–56.

[311] *Compare*, Hague (V), *supra* note 297 at art. 9; TALLINN MANUAL, *supra* note 291 R. 91, 92, at 250–51; United Nations Convention on the Law of the Sea, art. 2, 49, Dec. 10, 1982, 21 I.L.M. 1261 (1982) [hereinafter UNCLOS] (describing state sovereignty over various areas of the sea, including territorial and archipelagic seas, and the sovereignty rights associated therewith). The U.S. has not ratified the UNCLOS, but does consider some portions relating to overflight and transit passage regimes as customary international law. *See, e.g.*, President's Transmittal of the United Nations Convention on the Law of the Sea and the Agreement Relating to the Implementation of Part XI to the U.S. Senate with Commentary (Oct. 7, 1994), 34 I.L.M. 1393,

Under this approach, belligerent parties are prohibited from directing cyberspace operations either at, or from, cyberspace infrastructure within a neutral state.[312] However, there is a difference between a dedicated military communications facility, and the largely public infrastructure of the internet, a domain in which states generally do not bear responsibility for the acts of others.[313] To the extent that publicly available internet infrastructure passes through a neutral nation, and an effects based cyberspace operation travels through, but does not affect, that infrastructure, then this is not a violation of neutrality.[314] Absent any effects, there is no impact on the political independence of the neutral nation.[315] Thus, sovereignty of a non-belligerent nation would only be violated if there are effects in the physical and logical layers of cyberspace within that neutral nation's territory.[316]

These concerns demonstrate the complications posed by application of the TMA framework to cyberspace operations, contrasting sharply with the integrated cyberspace, information, and lethal capabilities presented by Chinese INEW. This tension will only be exacerbated as both Congress and the President have tasked DOD with developing, maintaining, and conducting offensive cyberspace operations.[317] Thus, while DOD is tasked as one of the primary U.S. instruments to conduct cyberspace operations, the congressional intelligence committees, other intelligence agencies, and scholars continue to express concern over the broad latitude granted DOD to exercise that primacy.

IV. Recommendations

In addition to articulating the factors that identify a particular military action as a TMA under the current statutory history-based framework, I recommend three policy changes. These policy changes would both simplify the application of the TMA exception, and ensure the decision-making and congressional oversight roles are effectively implemented. First is a modification of the existing TMA framework.

1405 (1995), *and*, Convention on International Civil Aviation, art. 3, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 [hereinafter Chicago Convention] (while the Chicago Convention generally applies to civil/commercial air travel, art. 3 indicates that state aircraft, including military aircraft, will not ordinarily fly over or land in the territory of another state without prior authorization).

[312] TALLINN MANUAL, *supra* note 289 R. 91, 92, at 250–51.

[313] Int'l Telecomm. Union (ITU) Library & Archive Serv., *Const. of the Int'l Telecomm. Union*, art. 33, 36, 48 (1992, as amended 1994, 1998, 2002, 2006, & 2010) [hereinafter *ITU Const.*]. The ITU is a United Nations agency which seeks to promote access to, and standards for the use of, telecommunications technologies. *See, e.g.*, ABOUT ITU. http://www.itu.int/en/about/Pages/default.aspx.

[314] TALLINN MANUAL, *supra* note 289, cmt. to R. 92, at 251.

[315] U.N. Charter, art. 2, para. 4.

[316] TALLINN MANUAL, *supra* note 289 R. 92, at 251.

[317] *See* NDAA 2012, *supra* note 78 at § 954 (providing congressional authorization to DOD for developing, maintaining, and conducting cyberspace operations); DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (2011) at 5 (discussing DOD's authority over cyberspace operations as directed by the President).

A. *Revise the Traditional Military Activities Framework*

The existing TMA framework is fraught with unnecessary complexity and ambiguity. A proposed three-element test to address these issues should be codified by statute. This revised test incorporates and consolidates three of the elements of the current TMA framework. Specifically, the proposed revision preserves the requirement that TMA be in support of a larger "overall operation" in which the U.S. role is apparent or acknowledged is preserved such that the exception will not swallow the rule. The revision also merges the requirement that an action be commanded by a military commander with the element that an action be conducted by military personnel. Both are subsumed under an element focusing on approval authorities and funding of an action. Additionally, the revision incorporates the "traditional" element, as it bears on whether a mission is authorized (or not prohibited) by Congress. However, the revised test discards the element requiring presidential or SECDEF approval in cases where hostilities are anticipated. Rather, a geographically based approach more accurately accounts for diplomatic risks arising from unacknowledged actions.

As a threshold matter, it is important to clarify whether the specific action is acknowledged or is intended to be acknowledged. That a particular action be unacknowledged is a necessary part of the covert action definition,[318] and the proposed test does not recommend any change to that definition. Thus, any specific action that is actually, or intended to be, acknowledged does not fit the threshold definition for covert action; as a result it is unnecessary to determine whether the TMA "exception" applies. Therefore, the proposed test only applies to specific actions that meet the threshold definition of "covert action" at 50 U.S.C. § 3093(e), and are not actually, nor intended to be acknowledged.

1. Test for Military Activities Inside of an AOH

As discussed, the covert action decision-making and reporting rules are about managing diplomatic risk. Thus, Congress has not required reporting of unacknowledged military activities that take place within an AOH. Rather, these actions are treated as pursuant to those overall hostilities.[319] While on a discrete level these actions may meet the criteria for "covert action," the management of risk indicates that these actions need not be subjected to the same oversight and accountability as those operations taking place outside of an AOH. Instead, Congress has appeared to acquiesce to a common sense position that regardless of U.S. acknowledgement, any specific actions within an AOH are pursuant to, or part of an acknowledged overall operation.[320] Military Information Support Operations, based on the effects that they are intended to have,[321] "take place"

[318] 50 U.S.C. § 3093(e).
[319] Chesney, *supra* note 57, at 543.
[320] *Id.* at 600.
[321] JP 3-13.2, *supra* note 205, at V-4–5.

wherever the target audience is located; therefore, this test applies to MISO operations aimed at a target audience within an AOH. For cyberspace MISO operations, the location of the target audience as either inside or outside of the AOH should be the deciding factor, because that is where cyberspace operations have effects.[322] Therefore, when a target audience is within an AOH, then the real question of whether a MISO or cyberspace operation is TMA is based on whether the military conducts the action. Thus, the following elements should apply.

The first element would require that both the specific action and the operators be funded by the DOD. As articulated previously, both the questions of whether the operation is commanded by a military commander, and the question of the military status of the operators, is essentially a funding question. This recognizes the oversight roles of Congress, and emphasizes the responsible committees' roles in exercising the power of the purse to check executive action.[323] This also simplifies the inquiry in an age where military and intelligence organizations operate side by side, and with significant overlap.[324]

This is particularly true in the cyber context where the NSA/CYBERCOM and DOD/Intelligence community overlap and convergence could frustrate more mechanistic approached focusing on the "military" status of particular personnel.[325] Thus, questions into the status of intermediate commanders and support personnel are ignored. These are irrelevant to the question of whether the particular program, or similar actions, will continue in the future; rather, the appropriate check is to eliminate funding for an agency to conduct a particular type of action in the future. In essence, this single inquiry subsumes the first two "elements" of the current statutory, history-based TMA inquiry.

The second element requires that the specific action is a mission either specifically authorized by Congress,[326] or a mission which Congress has not specifically prohibited. This bears upon the executive authority to unilaterally conduct the mission. With regard to the first category of missions, these actions fall within the maximum authority of the President to task the military.[327] The second category is within the "zone of twilight," where presidential power is perhaps uncertain.[328] However, the President's near plenary powers to act in

---

[322] There is of course the possibility that a target audience could be both inside and outside of the AO, in which case the second portion of the test for actions outside of the AO would apply.
[323] BAKER, IN THE COMMON DEFENSE, *supra* note 66 at 102.
[324] Schroen Interview, *supra* note 83; Nakashima, *supra* note 84.
[325] *See, e.g.*, 50 U.S.C. §§ 3301, 3326, 3327, 3607(d) (describing the various funding sources and rules for DOD intelligence activities and personnel, how these rules "nest" within the rules for the intelligence community as a whole, and requiring detailed reporting to Congress of any attempts to "reprogram" funds between programs or agencies).
[326] *See, e.g.*, 10 U.S.C. § 167(j). This statute provides a laundry list of potentially unacknowledged missions tasked to SOCOM. These include: direct action, unconventional warfare, foreign internal defense, MISO, counterterrorism, and several others.
[327] Youngstown Sheet & Tube, 343 U.S. at 635.
[328] *Id.* at 637.

foreign affairs provide that these types of actions are consistent with the exercise of presidential authority.[329] Furthermore, Congressional acquiescence to a historical pattern of military missions bolsters the contention that these actions are TMA.[330] This element bears on the statutory meaning of "traditional," in that it is a specified military mission authorized by Congress. Where Congress authorizes a mission, it should fall within the TMA scope regardless of historical precedent.

The final element is always met by MISO,[331] but could certainly apply to other operations as well. This requires that the contemplated action be in support of some larger actual or anticipated military operation in which the U.S. role is either apparent or acknowledged.[332] It is immaterial if that larger military operation is either anticipated, or ongoing, so long as the executive can point to some larger mission that a specific unacknowledged action supports. Failure to incorporate this element would provide an exception that swallows the rule, as all unacknowledged military actions could qualify as TMA so long as they were either (1) within an AOH, or (2) approved by the President or SECDEF.

By way of illustration, return to the hypothetical example of Chinese and U.S. tensions. Assume that the conflict has escalated to overt hostilities between the U.S. and China, and that mainland China is within the AOH. As part of the U.S. campaign against China, CYBERCOM has conducted a MISO operation targeting an audience within China, and this operation is ordered, commanded, and funded through military channels.[333] Under the existing TMA framework, this operation would qualify as a TMA because it is (1) commanded by a military commander (either the Commander, CYBERCOM or SECDEF), (2) is conducted by CYBERCOM personnel, and (3) is pursuant to ongoing hostilities, in which the U.S. role in the overall hostilities with China is apparent. This is uncontroversial, as was illustrated by the example of unacknowledged operations within Afghanistan.[334] This operation would also qualify under the proposed framework because it is (1) funded through military appropriations, (2) a type of mission authorized by Congress, and (3) is in support of the larger overall hostilities against China.[335] In neither case would it require approval of the

---

[329] *See, e.g.*, Curtiss-Wright, 299 U.S. at 319.

[330] Youngstown Sheet & Tube, 343 U.S. at 637. There is no evidence that Congress is not sufficiently aware of the types of unacknowledged military operations that could establish this type of historical precedent. The HASC and SASC appear informed, and satisfied with the degree of oversight they exercise, and the HPSCI and SSCI also appear aware that these actions take place, but desire more detailed reporting. This internal tension within Congress can be read as an internal balance, which equates to Congressional acquiescence.

[331] MISO are undertaken to influence opinions and actions "in a manner favorable to the originators objectives," and are thus always in support of some larger operation. JP 3-13.2, *supra* note 205 at I-1.

[332] S. REP. 102-85 at 44–48.

[333] For example, stemming from SECDEF, through the Commander, CYBERCOM.

[334] *See, e.g.*, Chesney, *supra* note 52, at 221–22.

[335] The DOD is authorized to conduct offensive cyberspace operations under § 954 of NDAA 2012, and is authorized to conduct MISO operations under 10 U.S.C. § 167(j).

specific action by either the President or SECDEF, as the effects are within the AOH.

These three elements, applicable to unacknowledged actions within an AOH, simplify application of the TMA exception in the cyber context. Rather than wading through the status of commanders and operators at NSA/CYBERCOM as "military" or not, focusing on DOD funding has two benefits. First, in light of restrictions on "reprogramming" or sharing funds between the military and intelligence communities,[336] it simplifies the inquiry into whether an operation is conducted by the military or by the intelligence community. Additionally, it allows the appropriate congressional committees (intelligence or armed services) to exercise their "power of the purse" to restrict similar operations in the future. In the climate of convergence where Navy SEALs conduct covert operations at the direction of the Director, CIA[337] a focus on funding will allow appropriate (and in most cases joint) oversight of military and intelligence activities. Furthermore, where both MISO and offensive cyberspace operations are tasked to DOD by Congress and the President, it strains credulity to require burdensome and mechanistic rules on the exercise of those capabilities when they target audiences and cyber-personas within an AOH. Rather, the military should have minimal constraints when conducting such actions.

2. Test for Military Activities Outside of an AOH

There is a significant difference in the diplomatic risk posed by unacknowledged cyber-MISO operations that target audiences outside of an AOH.[338] Thus, for cyber-MISO which targets audiences outside of an AOH, an additional requirement applies: simply that unacknowledged actions which seek to affect targets outside of an AOH must be approved by either the President or SECDEF. This requirement strengthens the risk management component of the

---

[336] *See, e.g.*, 50 U.S.C. §§ 3301, 3326–27.

[337] *See, e.g.*, Cooper, *supra* note 53. As the first element of the proposed TMA test requires that both the operators and the specific action be funded by DOD, it would appear that the raid to kill bin Laden would not qualify as a TMA. Where the raid was conducted under the command of CIA Director Panetta, the presumption would be that the CIA funded the action (for instance, by paying for logistics support, ISR assets, etc.) despite the fact that the DOD would have paid the pay and allowances of the operators. As a general rule the DOD provides support, and details personnel, to other agencies on a reimbursable basis. Thus, the cost of support to the CIA would be reimbursed to the DOD by the CIA. *See, e.g.*, 31 U.S.C. § 1535 (the "Economy Act"); U.S. DEP'T OF DEF., INSTR. 1000.17, DETAIL OF DOD PERSONNEL TO DUTY OUTSIDE THE DEPARTMENT OF DEFENSE, para. 3.b (Oct. 30, 2013) [hereinafter DODI 1000.17]. There are exceptions to this general rule, but these generally only apply where the function performed is one which is routinely performed by, or for the benefit of the DOD. DODI 1000.17, para. 3.b. Because the CIA is the default agency to perform covert actions, it does not appear that DOD support to a covert action would fall into the category of functions normally performed by, or for the benefit of the DOD. This judgment involves some assumptions as the author does not have access to the funding agreement for this particular action.

[338] Chesney, *supra* note 52, at 222.

current "anticipated hostilities" framework.[339] This is because diplomatic risks are posed by whether a targeted/impacted nation can expect to be targeted as opposed to U.S. intentions to acknowledge, or approve planning for an operation.[340] While not mitigating the risk posed for those actions actually executed outside of an AOH, it does reserve assessment and approval authorities to appropriately senior executive officials (the President and SECDEF), as opposed to a military commander.[341]

While the question of "outside of an AOH" is complicated in the cyber context, this is simplified in the MISO context where the location of the target audience, which is also the location of desired or expected effects, delineates the geographic "location" of the action. When dealing with other types of cyber operations, this is also a fairly straightforward question to answer,[342] and can most readily be answered by identifying the location of the target which an operation is expected or intended to affect. Thus, a cyberspace operation may have more than one location as the targets at the physical, logical, and cyber-persona level may not be co-located. Regardless, an "effects based" test for determining the "location" of a cyberspace operation provides a workable means to apply the proposed TMA framework that also accords with historical practice for radio and wire transmissions.[343]

In applying the hypothetical U.S. MISO contemplated above, assume the same command and funding parameters in the context of ongoing hostilities; however, this time assume that the MISO target audience is located in North Korea, outside of the AOH. This action would qualify under the current TMA framework.[344] Because this MISO is in support of ongoing hostilities, there is also no requirement that the specific action be approved by a national command

---

[339] S. Rep. 102-85 at 35.

[340] In both cases, the event which is tied to risk may never take place. An operation can be "intended" to be acknowledged, but never actually be acknowledged. Additionally, the President or SECDEF may approve operational planning for an operation which either never takes place, or is so far in the future in relation to a current unacknowledged operation as to bear no reasonable relation to that future operation from the perspective of anyone outside of the U.S. military or the executive branch. In either case, there is no way that the targeted nation could expect to be the target of such an operation.

[341] This also mirrors a policy requirement for National Command Authority approval for lethal actions outside of an acknowledged AOH, apparently implemented by Secretary of Defense Robert Gates. Chesney, *supra* note 57, at 575, 606 (citing to ERIC SCHMITT & THOM SHANKER, COUNTERSTRIKE: THE UNTOLD STORY OF AMERICA'S SECRET CAMPAIGN AGAINST AL QAEDA 118–119 (2011)).

[342] Franzese, *supra* note 270, at 5; Nguyen, *supra* note 296, at 1084.

[343] These types of operations may have effects on some unintended third party. It is not clear that the Law of Armed Conflict/Law of War is implicated, but impacts on an unintended third party or neutral state may properly be assessed in relation to the military advantage to be gained from the MISO operation under the LOAC principle of proportionality. *See, e.g.*, AP I, *supra* note 292, art. 51(5)(b); *see also* Hague (V), *supra* note 297, art. 8–9.

[344] S. Rep. 102-85 at 44–48.

authority (the President or SECDEF).[345] This fails to ensure executive responsibility in the case of diplomatic risk in North Korea. This risk is governed by North Korean expectations, not whether there are ongoing hostilities in some other nation.[346] Under the proposed TMA framework, this action would need to be approved by national command authority in order to qualify as TMA. This provides a superior means of ensuring executive accountability for diplomatically risky actions that take place, or have intended effects, outside of a theater of ongoing hostilities. Thus, the requirements for actions having effects outside of an AOH ensure greater executive accountability and congressional oversight than those which take place pursuant to "anticipated" hostilities.

There may be concerns that the proposed exception is too broad, and that it will enable all military operations to be classified as TMA, thereby failing to address current Congressional concerns over the scope of unreported military activities; however, these fears are unfounded. First, the requirement that the overall operation is "to be" acknowledged doesn't actually require acknowledgment,[347] but only an intent to do so at some indeterminate time in the future. This is especially problematic for "anticipated" hostilities that may never take place. Thus, acknowledgment of some "anticipated operation" is a poor trigger for identifying diplomatic risk under the current TMA rubric, and the appropriate focus should be on the location of an action with respect to ongoing hostilities.[348]

Furthermore, there are two factors that will ensure that the scope of military missions does not grow too broad. First, the CIA is the default federal agency for the conduct of covert operations, and only the President can designate any other agency to conduct covert activities.[349] Furthermore, the proposed geographic trigger for National Command Authority approval for any unacknowledged military actions outside of an AOH requires that either the President or SECDEF must approve any such actions. This contrasts with the current TMA exception which enables a military commander to approve this type of action without presidential or SECDEF approval or notification. Second, the revised test would carry over the current requirement that TMA be pursuant to a larger acknowledged military mission. Thus, the military will never be able to unilaterally conduct an unacknowledged action outside of an AOH. Nor could the military ever conduct an independent unacknowledged action unless it is categorized as a covert action, and subject to the applicable decision-making and congressional reporting requirements.[350]

---

[345] *Id.* at 46–47.
[346] Anderson, *supra* note 163.
[347] Wall, *supra* note 50, at 130.
[348] Anderson, *supra* note 163, at 15. *See also*, Kirkpatrick et. al., *supra* note 172.
[349] E.O. 12333, *supra* note 81, at ¶ 1.7(a)(4).
[350] *Id.*; S. REP. 102-85 at 44–48; 50 U.S.C. § 3093.

A geographic distinction for TMA that must be approved by the President or SECDEF represents a simpler, more effective way to ensure the apparent nature of the U.S. role, and to ensure that diplomatic risks are assessed by appropriately senior executive officials. Under the proposed test, where the U.S. is engaged in ongoing hostilities, then specific actions within the AOH are TMA and exempt from the covert action rules. For those actions outside of the AOH, where the specific action is not intended to be acknowledged, then the risk posed by this operation is independent of whether there is some putative "overall operation" in a geographically distant nation or that has yet to take place. The diplomatic risk turns on whether the affected nation can reasonably expect to be the target of a U.S. action. Thus, outside of an AOH, whether hostilities are "anticipated" is irrelevant from the perspective of the targeted nation. In cases of anticipated hostilities, the fact is that there are no current hostilities to point to, and thus no expectation of being targeted. While not providing any additional mitigation of diplomatic risk over the old TMA framework for unacknowledged actions outside of an AOH, the proposed framework requires National Command Authority approval for those actions, thereby restricting the assessment and approval for those actions to senior executive officials better posed to assess diplomatic risk than military commanders. The proposed test will require presidential or SECDEF accountability for such actions, as well as result in increased accountability for actions outside of an AOH that have negative diplomatic consequences. In addition, with the proposed requirements for greater detail in SAP reporting which follow, this creates a near mirror of the process for covert actions in which TMA outside of an AOH will be approved by National Command Authority, and reported to Congress in greater detail.

There may be additional concerns about congressional oversight; however, regardless of whether they are acknowledged, these actions are still subject to oversight by the Armed Services Committees.[351] The element requiring that an operation be in support of a larger acknowledged military operation will result in no less oversight than under the current regime. Any unacknowledged military actions that are not in support of a larger military operation could not qualify as TMA. Additionally, this test preserves the concept of executive accountability for diplomatically risky actions abroad. Specifically, the President or SECDEF must approve specific unacknowledged operations outside of an AOH. This mirrors the current framework in which the President or SECDEF must approve both the operational planning for the overall operation (such as the actual hostilities in a theater of ongoing hostilities), as well as the specific unacknowledged action.

This revised three-element test captures the essence of the concerns over current unacknowledged military activities through preservation of both congressional oversight, and assurance of presidential accountability for diplomatically risky actions outside of an AOH. The next two recommendations

[351] DODD 5205.07, *supra* note 92; Chesney, *supra* note 57, at 611, 613; Wall, *supra* note 50, at 103–04.

address additional concerns related to the degree of congressional oversight and executive accountability.

B. *Improved Reporting to the House and Senate Armed Services Committees*

The congressional intelligence committees are concerned about the limited oversight they have over unacknowledged military activities.[352] However, as discussed, it is the Armed Services committees that have a more appropriate role and authority to exercise oversight over military actions. To enable congressional oversight, Professor Chesney argues that the DOD should report with a greater degree of specificity on SAP programs and other unacknowledged military activities to the Armed Services committees.[353]

The following are more focused recommendations that bear upon the type of MISO and cyberspace operations contemplated herein. The Department of Defense should implement policies to provide for detailed reporting to the Armed Services Committees on the following categories of cases: unacknowledged operations in support of intelligence community, or Title 50 agencies; certain classes of operations which seek to influence conditions abroad; and funding to either of these types of operations. It is this goal of influencing conditions that is both the critical piece of unacknowledged operations abroad, and that which poses the greatest risk.[354]

Military Information Support Operations are squarely within this class of operations as they are employed to influence actions in a target audience,[355] and the fallout from identifying the U.S. as the messenger could negatively impact U.S. interests. Improved reporting on support to the intelligence community provides clarity on the convergence trend, reinforces the understanding of Congress regarding the reality of conditions on the ground, and allows the Armed Services and Intelligence Committees to coordinate their oversight efforts, to the extent that they are inclined to do so.

C. *Document Intent to Acknowledge*

The executive branch reporting exception for unacknowledged actions which are intended to be acknowledged has also been addressed.[356] The trigger for whether an operation is "covert" is whether the action is actually, or intended to be, acknowledged.[357] The Department of Defense should implement a policy whereby the intent to acknowledge any specific action is documented

---

[352] H. R. REP. NO. 111-2701 at 50; Gertz, *supra* note 88.
[353] Chesney, *supra* note 57, at 543.
[354] Wall, *supra* note 50 at 129; Chesney, *supra* note 57, at 589.
[355] JP 3-13.2, *supra* note 205, at V-4.
[356] 50 U.S.C. § 3093.
[357] 50 U.S.C. § 3093(a).

contemporaneously with the authorization of that action. This documentation should include a clear statement that the U.S. Government intends to acknowledge its role in the action, and whether that intent applies at the time of the action or at some specified future time. If the intent is to acknowledge at some future time, then the documented intent should specify any temporal or factual conditions precedent that must be met in order to either announce, or acknowledge the operation. In this way, there will always be a clear indicator of whether, and in what circumstances, an unacknowledged military activity will be acknowledged. This will also provide a clear indication of why a particular unacknowledged operation may not have been reported to Congress as a covert action.

Conclusion

The current Traditional Military Activities exception to the covert action decision-making and congressional oversight rules is complicated and ambiguous. This ambiguity constrains U.S. military initiative, thereby hampering the ability of U.S. forces to combat emerging threats in the cyber domain. This confusion starts with the current test for Traditional Military Activities.[358] This framework is outdated in light of convergence, and in its mechanistic approach, which fails to recognize the difference between hostilities within an AOH, hostilities outside of an AOH, and the relative diplomatic risks they pose.[359]

However, the current framework is subject to a straightforward, common sense analysis. By focusing on issues such as funding and authorities, the questions regarding what it means to be commanded by a military commander and to be carried out by military personnel are simplified. Furthermore, the focus on the instruments by which military force is authorized informs the geographic scope the AOH. If one recognizes the presidential authority to act in foreign affairs, and Congress' power to check executive action, the statutory and executive instruments that establish the AOH are easily identified. There is also little role for historical precedent, particularly in the cyber domain.

If Congress authorizes a particular military mission, then Congress is powerless to argue that the President does not have broad authority to employ the military in that mission as he sees fit.[360] Furthermore, despite the military's "traditional" practice of applying LOAC to all military operations, these restrictions do not encompass cyberspace operations that lack physical or lethal effects. Thus, MISO are generally unconstrained by LOAC, regardless of the nature of the overall operation. The Law of Armed Conflict generally only applies to those cyberspace operations which have physical effects, not those which are purely informational or intelligence gathering.[361] Cyberspace operations also do

[358] S. REP. 102-85 at 44–48.
[359] Chesney, *supra* note 52, at 222.
[360] Youngstown Sheet & Tube, 343 U.S. at 635.
[361] TALLINN MANUAL, *supra* note 289, R. 91-95, at 250–56.

not violate sovereignty or neutrality of non-belligerent states absent effects in those nations.[362] Rather, akin to radio and wire telegraphy regimes, a cyberspace operation must have effects within the territory of a nation to have any impact on that nation's sovereignty.[363]

The proposed test for TMA accounts for the reality of convergence, and maintains the power of Congress to exercise its oversight authority.[364] If an activity is funded by the military, then the appropriate oversight committees are the Armed Services Committees, incorporating a degree of shared oversight alongside the intelligence committees for agencies like the NSA, which are part of both the DOD and intelligence community.[365] This focus on funding is the crux of the inquiry into what it means for an activity to be commanded and conducted by military personnel.[366]

Additionally, concentrating on the second element and whether the mission is one authorized, explicitly or implicitly, by Congress moves away from the focus on historical precedent, which is complicated in its application to cyberspace. It also fits neatly into the accepted analytical framework for executive power in the separation of powers context.[367] Finally, the distinction between ongoing and anticipated hostilities is mechanistic and moot in that those unacknowledged activities with effects inside an AOH are not subject to the normal covert action rules.[368] So long as the activity is in support of some larger acknowledged operation, then the true risk is posed by whether a nation can expect to be targeted by some unacknowledged U.S. military activity.

Therefore, the focus should be on the geographic location of an activity with respect to an AOH. For those activities that are intended or expected to have effects outside of an AOH, there should be the additional requirement that they be approved by either the President or SECDEF. These three elements maintain the decision-making, and congressional oversight roles for diplomatically risky actions without focusing on distinctions that have nothing to do with those concerns; however, the pressure for increased oversight will surely continue.[369]

More detailed reporting to the Armed Services Committees for certain types of actions recognizes the risk posed by actions that are intended to influence conditions abroad, and Congress's interest in oversight over those actions.[370] The reporting of support to intelligence community, or Title 50, agencies also

---

[362] Hague (V), *supra* note 297 art. 9; TALLINN MANUAL, *supra* note 291, R. 92, at 251–52.
[363] Hague (V), *supra* note 297, art. 9
[364] BAKER, IN THE COMMON DEFENSE, *supra* note 66, at 102.
[365] E.O. 12333, *supra* note 81; Wall, *supra* note 50, at 103–04.
[366] Wall, *supra* note 50, at 107.
[367] Youngstown Sheet & Tube, 343 U.S. at 635–37.
[368] Chesney, *supra* note 52, at 223.
[369] H. R. REP. NO. 111-2701 at 50; Emptywheel, *supra* note 83; Nakashima, *supra* note 84.
[370] Chesney, *supra* note 52, at 223.

recognizes the reality of convergence, thereby, allowing congressional coordination on oversight.[371] Implementing more robust reporting on the funding of these types of operations will also enable Congress to exercise its "power of the purse" to hold the executive accountable and check unacceptable executive action.[372]

All authorizations for unacknowledged actions that are intended to have effects outside of an AOH should include a contemporaneous recording of whether and when the U.S. role in the specific action will be acknowledged. This contemporaneous recording of intent will ensure that even though an action remains unacknowledged it can still fit within the current TMA framework, while still preserving the executive branch's ability to justify to Congress why a particular action may not have been reported.[373] Recording the conditions precedent to acknowledgment will also clarify the left and right limits for individual personnel, so that they are entirely clear on when an action may be acknowledged, or why an action has not yet been acknowledged.

The intent of the proposed TMA analytical framework is to provide clarity to operators. This clarity is needed to enable action and initiative to combat the cyber threats posed by rising powers with developed, mature doctrines aimed at defeating the United States. Additionally, the recommendations provide a revised TMA framework that is greatly simplified, define a more coherent approach to identifying diplomatic risk, increase presidential accountability for those risks, and ensure that Congress retains an appropriate degree of oversight.

[371] Chesney, *supra* note 57, at 545, 562–63, 578–79.
[372] BAKER, IN THE COMMON DEFENSE, *supra* note 66, at 102.
[373] 50 U.S.C. § 3093.