**MILITARY LAW REVIEW**

**Volume 229** **Issue 3**

# THE RISE OF THE "FIFTH FIGHT" IN CYBERSPACE: A NEW LEGAL FRAMEWORK AND IMPLICATIONS FOR GREAT POWER COMPETITION

MAJOR LAURA B. WEST*

## I. Introduction

America's perspective of the global security environment significantly changed after the discovery of the Russian interference in the 2016 U.S. presidential election.[1] Agencies charged with securing the Nation were left to question decades of presumed defense and security superiority.[2] Government decision-makers rushed to shift U.S. national security priorities from a focus on global terrorists to a focus on a handful of great powers.[3] America quickly found itself in the center of an ongoing and "new"—yet

* Judge Advocate, U.S. Army. Presently assigned as Deputy Chief of National Security Law, U.S. Cyber Command, Fort Meade, Maryland. LL.M., National Security Law, 2020, Georgetown University Law Center, Washington, D.C.; LL.M., Military Law with Criminal Law Concentration, 2016, The Judge Advocate General's Legal Center and School, Charlottesville, Virginia; J.D., 2010, William and Mary Law School, Williamsburg, Virginia; B.S., 2004, United States Military Academy, West Point, New York. Previous assignments include Assistant Executive Officer of the U.S. Army Legal Services Agency and Chief Commissioner, U.S. Army Court of Criminal Appeals; Regimental Judge Advocate, 160th Special Operations Aviation Regiment (Airborne); Trial Counsel (Prosecutor) and Chief of Administrative and Civil Law, Fort Carson; Chief of International & Operational Law, Afghanistan and Fort Riley; Brigade Judge Advocate, Fort Riley; Military Intelligence Company Executive Officer, Hawaii; Signals Intelligence Team Officer-in-Charge, Joint Special Operations Task Force-Philippines; and Staff Intelligence Officer, Schofield Barracks, Hawaii. The views expressed in this article are those of the author in her personal capacity and should not be understood to represent those of the Department of the Army or any other U.S. Government entity.

[1] *See generally* S. REP. NO. 116-290, at 159–202 (2020); *cf.* U.S. DEP'T OF DEF., SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA 2–3 (2018) [hereinafter 2018 U.S. DEFENSE STRATEGY SUMMARY].

[2] *E.g.*, *id.* at 159; 2018 U.S. DEFENSE STRATEGY SUMMARY, *supra* note 1, at 3.

[3] *See* JIM SCIUTTO, THE SHADOW WAR: INSIDE RUSSIA'S AND CHINA'S SECRET OPERATIONS TO DEFEAT AMERICA 10 (2019).

wholly recognizable—type of international conflict.[4] While this conflict and the resulting shift in national security priorities seemed sudden to some, portions of the U.S. defense apparatus engaged in intelligence and cyberspace operations had already been working for years to address this nascent conflict.

The unclassified synopsis of the 2018 U.S. National Defense Strategy labels this emergent conflict as "strategic competition," also known as "great power competition," and surmises that this "[i]nter-state strategic competition, not terrorism, is now the primary concern in U.S. national security."[5] Defining the scope of this conflict presents its own challenges, though. To begin, it is not "war" in the traditional sense. The United States is not engaged in armed conflict with any great power adversary. Instead, conflict is waged with adversaries below the threshold of armed conflict, involving "persistent engagement" and countering malicious activity in the shadows.[6] As a result, covert action—commonly referred to as the "fifth function"[7]—has emerged as an obvious principal means of action.

---

[4] *See id.* at 10–13.

[5] 2018 U.S. DEFENSE STRATEGY SUMMARY, *supra* note 1, at 1; *see* EXEC. OFF. OF THE PRESIDENT, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 2–3 (2017) (describing it as "political, economic, and military competitions" that are "intertwined, long-term challenges that demand our sustained national attention and commitment" with sides neither at war nor at peace). Adversaries such as Russia and China also recognize this new state of conflict. *See, e.g.*, ANTHONY H. CORDESMAN, CHINA'S NEW 2019 DEFENSE WHITE PAPER: AN OPEN STRATEGIC CHALLENGE TO THE UNITED STATES, BUT ONE WHICH DOES NOT HAVE TO LEAD TO CONFLICT 1 (2019) (citing China's defense strategy, which states that "international strategic competition is on the rise").

[6] *See, e.g.*, SCIUTTO, *supra* note 3, at 11; LYLE J. MORRIS ET AL., GAINING COMPETITIVE ADVANTAGE IN THE GRAY ZONE: RESPONSE OPTIONS FOR COERCIVE AGGRESSION BELOW THE THRESHOLD OF MAJOR WAR, at ix (2019). In 2018, U.S. Cyber Command announced its concept for persistent engagement to address shifting national security priorities in great power competition. U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY (2018); *see* Jacquelyn G. Schneider, *Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy*, LAWFARE (May 10, 2019, 8:00 AM), https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

[7] The "fifth function" is a reference to a famously vague and open-ended provision in the National Security Act of 1947 (enumerated as the fifth provision outlining activities of the CIA) that implied the Central Intelligence Agency (CIA) could engage in "other activities related to intelligence which the President may direct," which came to be interpreted—whether intended or not—as authority for covert action by the CIA. Robert Chesney, *More on CIA Drone Strikes, Covert Action, TMA, and the Fifth Function*, LAWFARE (Sept. 7,

Adversaries in this new conflict also look different but familiar. Generally, they no longer take on the title of non-state actor or terrorist organization, as was the case for the past two decades. Rather, adversaries include other great powers such as Russia and China, as well as rogue regimes such as North Korea and Iran.[8] The Department of Defense (DoD) specifically identified these countries as the four main threats the United States must counter in great power competition.[9]

While adversarial goals in great power competition seem to echo the Cold War, in that adversaries strive to undermine U.S. power and sow discord in the American democratic way of life, this shadow war brought with it new and ever-changing tactics.[10] Cyberspace and information operations surfaced as the tactics of choice among adversaries, mostly due to the rapid growth of new technology,[11] the rise of a novel information environment with increasingly virulent effects,[12] and the shifting character

---

2014, 6:16 PM), https://www.lawfareblog.com/more-cia-drone-strikes-covert-action-tma-and-fifth-function.

[8] *See, e.g.*, MORRIS ET AL., *supra* note 6, at 6; 2018 U.S. DEFENSE STRATEGY SUMMARY, *supra* note 1, at 2; U.S. DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018) [hereinafter DOD CYBER STRATEGY SUMMARY].

[9] *See* DOD CYBER STRATEGY SUMMARY, *supra* note 8, at 3; *see also* Greg Myre, *'Persistent Engagement': The Phrase Driving a More Assertive U.S. Spy Agency*, NPR (Aug. 26, 2019, 2:41 PM), https://www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency; Fred Dews, *Joint Chiefs Chairman Dunford on the "4+1 Framework" and Meeting Transnational Threats*, BROOKINGS (Feb. 24, 2017), https://www.brookings.edu/blog/brookings-now/2017/02/24/joint-chiefs-chairman-dunford-transnational-threats.

[10] *See* SCIUTTO, *supra* note 3, at 11; MORRIS ET AL., *supra* note 6.

[11] *See* 2018 U.S. DEFENSE STRATEGY SUMMARY, *supra* note 1.

[12] *See* P.W. SINGER & EMERSON T. BROOKING, LIKEWAR: THE WEAPONIZATION OF SOCIAL MEDIA 18 (2018) (discussing social media giving rise to a new information "battlespace," signaling the shifting power dynamic and control platform providers wield over users and nations through their algorithms). The extraction and exploitation of data, private surveillance of human activities, and the weaponization of civil society is quickly becoming the new normal for navigating the world as the Nation shifts from an industrial-era economy into the emerging informational economy. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 12 (2019) (suggesting that surveillance capitalism is unprecedented in our times); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 37 (2019); *cf.* Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 89 (2016) (describing a "digital platform revolution," causing a "paradigmatic shift in the ways we produce, consume, work, finance, and learn"). In 2017, the Supreme Court added to this idea of a novel information environment when it identified the most important place (in a spatial sense) for the exchange of views today to be "cyberspace . . . and social media in particular." Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017).

of war.[13] As a result, while this conflict is fought in all five domains of warfare (i.e., air, sea, land, space, and cyberspace), a high concentration of U.S. defense and security efforts remain within the ever-evolving "fifth domain" of cyberspace.[14] Confirming this state of the security environment, General Paul Nakasone, Commanding General of U.S. Cyber Command and Director of the National Security Agency (NSA), stated in a 2018 speech that "[t]he environment we operate in today is truly one of great power competition, and in these competitions, the locus of the struggle for power has shifted towards cyberspace."[15]

The emergence of this great power competition finally forced the inevitable collision of the two "fifths"—covert action and cyberspace operations. National security practitioners expected this collision for some time due to their keen awareness that the fifth function and the fifth domain emerged and operated in parallel, often intersecting, uncertain legal architectures since their inceptions. Over the span of more than a decade, covert actions and cyberspace operations increasingly crossed paths,[16] an expected occurrence since cyberspace operations most often require covert

---

[13] *Cf.* 2018 U.S. DEFENSE STRATEGY SUMMARY, *supra* note 1, at 3.

[14] Cyberspace became colloquially known as the "fifth domain" when it took its place as a recognized domain of warfare by the U.S. Department of Defense. JOINT CHIEFS OF STAFF, NATIONAL MILITARY STRATEGY OF THE UNITED STATES OF AMERICA 16 (2004).

[15] *Gen. Nakasone Lays out Vision for '5th Chapter' of U.S. Cyber Command*, MERITALK (Sept. 7, 2018, 2:41 PM), https://www.meritalk.com/articles/nakasone-cyber-command-vision (quoting General Paul Nakasone). Ironically, General Nakasone further claimed that this shift to great power competition in cyberspace involved U.S. Cyber Command writing its "fifth chapter" of the command's history. *Id.* The four preceding chapters included goals of creating layered protections, protecting critical infrastructure, building new defensive capabilities, and combating ISIS propaganda. *Id.*

[16] Arguably, the focus on cyber operations started as early as 1999 under the Clinton administration but gained significant momentum under the Obama administration in the wake of the Estonia attacks of 2007. *See* RICHARD A. CLARKE & ROBERT K. KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS 3–4 (2019); *cf.* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, at xxiii (Michael N. Schmitt ed., 2d ed. 2017); CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE, at v (2009) (advocating for the work that needed to be accomplished to change the Nation's cybersecurity approach that "over the past 15 years ha[d] failed to keep pace with the threat"); *The Comprehensive National Cybersecurity Initiative*, WHITE HOUSE, https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (last visited Sept. 27, 2021).

action and strongly resemble intelligence activities.[17] The resulting intersection between the legal frameworks governing covert action and cyberspace operations created what is referred to as the "fifth fight."

This article focuses on the fifth fight: the conduct or fight taking place through covert or "secret" cyber operations today. The term is also an acknowledgment of its foundations or the underlying interagency fight for authorities to conduct these cyber operations. In an era of great power competition, this fifth fight forced significant changes to the governing domestic legal framework, which has notable implications for the future nature of conflict, accountability, and responsibility by the United States.

Beginning with a historical background, Part II outlines the development of the covert action legal framework. The first half of that part addresses the important background behind the internal Government fight for authorities, which stems from the proverbial Title 10/Title 50 debate.[18] This part ends with a discussion of how the covert legal framework and fight for authorities have placed cyberspace operations on precarious and uncertain legal footing when entering today's shadow war of great power competition.

Part III addresses how the rise of great power competition forced the creation of more legal certainty. Significantly, Congress recently passed legislation to address the fifth fight. The National Defense Authorization Acts (NDAAs) for fiscal year (FY) 2019[19] and FY 2020[20] contained covert or "clandestine" cyber operations provisions that largely evaded public comment outside of national security circles. The legislation was meant to clarify authorities and put an end to the interagency dispute[21] and now allows for greater cyberspace freedom of movement to address the threats

---

[17] *See* Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SEC. L. & POL'Y 539, 580–81 (2012); Andru E. Wall, *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action*, 3 HARV. NAT'L SEC. J. 85, 121 (2011). *See also* Gary D. Brown & Andrew O. Metcalf, *Easier Said than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SEC. L. & POL'Y 115, 117–18 (2014).

[18] *See* discussion *infra* Section II.B.2.

[19] National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1632, 132 Stat. 1636, 2123 (2018) (codified at 10 U.S.C. § 394).

[20] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1631(b)–(c), 133 Stat. 1198, 1742 (2019) (codified at 10 U.S.C. § 397 note).

[21] *See* H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.).

the United States faces in strategic competition. Such freedom of movement comes at a price, with less oversight and public accountability. Congress, and many within the executive agencies involved in the fight for authorities, claim that these changes and the associated costs merely acknowledge the current state of cyberspace operations and what is required to keep pace with America's competitors. Challenging this claim, Part III provides further analysis of these legislative provisions and their immediate implications on the cyber legal framework and expounds on what these developments might mean for the future of great power competition or deterrence in cyberspace.

These seemingly minor affirmations regarding the legal structure created sweeping changes, despite not being readily recognizable today. While these changes resolved some ambiguity in the legal framework to allow the U.S. military to counter and deter threats in cyberspace more actively and effectively,[22] this article shows that they created even more questions and concerns about the nature of conflict, the accountability and responsibility for these operations, and the ability to secure an open and free cyberspace. Part IV addresses these pressing issues and the United States' role in shaping the future of international conflict by offering proposals and key considerations for the future of the fifth fight in great power competition.

## II. The Rise of the Fifth Fight

### A. The Fifth Function: Building the Legal Framework

#### *1. Laying the Groundwork for the Fifth Function*

The "fifth function," now synonymous with the term "covert action," is deeply rooted in America's national security framework. Most trace the concept's birth to a National Security Act of 1947 provision that directed the newly minted Central Intelligence Agency (CIA) to "perform such other functions and duties related to intelligence affecting the national security

[22] *Hearing on U.S. Special Operations and Cyber Commands in Review of the Defense Authorization Request for Fiscal Year 2022 and the Future Years Defense Program Before the S. Comm. on Armed Servs.*, 117th Cong. 58 (2021) [hereinafter Statement of General Nakasone] (statement of General Paul M. Nakasone, Commander, U.S. Cyber Command) (noting that the enactment of these cyber authorities have moved U.S. Cyber Command "from being a static to a very active force").

as the National Security Council may from time to time direct."[23] The provision links U.S. Government covert action to intelligence community activities vice military activities. As a result, the CIA historically conducted, and zealously guarded, covert activities.

The National Security Act and the resultant establishment of the CIA was the U.S. Government's attempt to reorganize foreign policy and military establishments; it was a clear reaction to the early developments of the Cold War and lessons learned from World War II.[24] By authorizing the fifth function, Congress provided the CIA—a civilian intelligence agency that would report directly to the President—with the flexibility to meet the unforeseen challenges of the looming Cold War.[25]

Covert action by the CIA established its foothold in American foreign policy during the Cold War. During the early stages of the conflict, the State Department advised the National Security Council (NSC) that Soviet covert operations threatened to defeat American foreign policy objectives.[26] The NSC found covert psychological operations necessary to supplement foreign information activities to counter the Soviet Union's "vicious psychological efforts" and pinned the rose on the CIA as the "logical agency to conduct such operations."[27] As the Soviet threat grew, the NSC expanded the range of covert activities to include "economic warfare, sabotage, subversion against hostile states (including assistance to guerrilla and refugee liberation groups), and support of indigenous anti-communist

---

[23] National Security Act of 1947, Pub. L. No. 80-253, § 102(d)(5), 61 Stat. 495, 498; *see* STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 549 (6th ed. 2016). *But see U.S. Intelligence Agencies and Activities: Risks and Control of Foreign Intelligence, Hearings Before the H. Select Comm. on Intel.*, 94th Cong. 1729, 1732–33 (1976) [hereinafter Rogovin Memorandum] (statement of Mitchell Rogovin, Special Couns. to the Dir. of Cent. Intel.) (explaining that the concept of covert actions dates back to the first century of the Nation's existence when over 400 covert special agents were appointed by the President to influence foreign policy).

[24] *National Security Act of 1947*, U.S. DEP'T OF STATE, https://history.state.gov/milestones/1945-1952/national-security-act (last visited Sept. 28, 2021); *see 1945–1952: The Early Cold War*, U.S. DEP'T OF STATE, https://history.state.gov/milestones/1945-1952/foreword (last visited Sept. 28, 2021).

[25] 1 S. REP. NO. 94-755, at 475 (1976).

[26] *Id.* at 490; *see generally* Memorandum from George F. Kennan to Nat'l Sec. Council, subject: The Inauguration of Organized Political Warfare (Apr. 30, 1948).

[27] 1 S. REP. NO. 94-755, at 490–91.

elements in threatened countries."[28] Consequently, the CIA's covert action became the foremost form of addressing foreign threats during this era of conflict conducted below the threshold of armed conflict.[29]

Following almost thirty years of covert action conducted under the guise of the fifth function authority and legislative acquiescence,[30] the CIA became the primary agency for covert action. Covert actions by the CIA—the justification for which changed sharply during this period of time[31]—took on various forms throughout history, from "barely more intrusive than diplomacy to large-scale military operations."[32] The CIA subsequently came to broadly define covert action as any "clandestine activity designed to influence foreign governments, events, organizations, or persons in support of the United States foreign policy conducted in such a manner that the involvement of the U.S. Government is not apparent."[33] Although covert actions took on a wide range of activities under this definition, all were "plausibly deniable" by the U.S. Government.[34]

In contrast, covert actions were not historically meant to include "armed conflict by recognized military forces, espionage and counterespionage, nor cover and deception for military operations."[35] Obviously, this excluded

---

[28] *Id.* at 490; *see* NSC 5412/2, *reprinted in* U.S. Dep't of State, Foreign Relations of the United States, 1950–1955, at 746 (Douglas Keane et al. eds., 2007) [hereinafter NSC 5412/2] (stating that in the interests of world peace and U.S. national security, covert operations should supplement the overt foreign activities of the U.S. Government). At the time, National Security Directive 5412/2 defined covert operations as "all activities conducted pursuant to this directive which are so planned and executed that any U.S. Government responsibility for them is not evident to unauthorized persons and that if uncovered the U.S. Government can plausibly disclaim any responsibility for them." *Id.* at 748. While the directive provided a list of activities considered to be cover action, it specifically stated that "[s]uch operations shall not include: armed conflict by recognized military forces, espionage and counterespionage, nor cover and deception for military operations." *Id.*

[29] *See generally* 1 S. REP. NO. 94-755, at 50. A 1954 report on CIA activities cited in the famous Church Committee reports reflects the general understanding that the CIA stepped up as the agency leading covert action, associated with human intelligence, below the threshold of war. *Id.*; *see* DYCUS ET AL., *supra* note 23, at 551.

[30] Chesney, *supra* note 17, at 587.

[31] 1 S. REP. NO. 94-755, at 57 ("The justification for covert operations has changed sharply, from containing International (and presumably monolithic) Communism in the early 1950s to merely serving as an adjunct to American foreign policy in the 1970s.").

[32] DYCUS ET AL., *supra* note 23.

[33] 1 S. REP. NO. 94-755, at 475.

[34] *Id.*

[35] *See generally* NSC 5412/2, *supra* note 28.

all overt operations conducted openly by the United States, from initial planning to execution. Further, *clandestine* military actions became distinguishable in that such actions might be initially secret (typically for operational security reasons), but the United States intended to reveal its role and the existence of those operations when complete or discovered prematurely.[36]

These definitions and attendant distinctions have generally held firm throughout the development of the covert action legal framework, with the exception of the nuanced distinction Congress recently made between military clandestine and covert cyber and information operations.[37] Nonetheless, these definitions, distinctions, and associated actions form the basis for the consternation and debate between Congress, the executive, and various executive branch agencies that has carried on to this day.

*2. Defining Covert Actions and Balancing Power: Congressional Oversight and Reform*

As the fifth function rooted itself in the fabric of the American national security framework, especially as the operation *du jour* in conflict below the threshold of armed conflict, so too did it start to find its opposition. After multiple decades of unfettered action by the intelligence agencies, Congress began to question covert action authorities and oversight. Congress found itself forced to take action in light of mounting governmental abuses, including Cold War covert tactics, domestic espionage during the Vietnam War period that undermined U.S. citizens' rights across the board,[38] covert action in Latin America, and the Watergate scandal that involved domestic

[36] S. REP. NO. 101-358, at 51 (1990); Wall, *supra* note 17, at 138.
[37] *See* 10 U.S.C. § 394; National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1631(b)–(c), 133 Stat. 1198, 1742 (2019) (codified at 10 U.S.C. § 397 note). *See also* discussion *infra* Sections III.B.2., III.C.2.
[38] *See* Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES, Dec. 22, 1974, at A1; LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 4–9 (2016) (discussing domestic surveillance scandals investigated by the Pike and Church Committees that had sweeping implications on the rights of individuals); *see also* DYCUS ET AL., *supra* note 23, at 507. Mostly, domestic spying was conducted under the direction of the National Security Agency (NSA), which also used covert action at the time without public knowledge or legislative establishment. *Id.*

covert action.[39] Legislators, typically asking few questions about covert operations for political self-preservation,[40] were finally pressured by the press and the public to investigate and create checks on covert operations and other intelligence activities.[41]

The first in a series of congressional checks on covert action came by way of the 1974 Hughes-Ryan Amendment.[42] Using the power of the purse, Congress made it impermissible for funds to be spent "by or on behalf of the [CIA] . . . unless and until the President finds that each such operation is important to the national security of the United States."[43] This requirement became known as a "presidential finding." The requirement arguably provided an incredibly vague standard that was unlikely to face much resistance from Congress once presented by the President.[44] Nonetheless, Congress intended for such a finding to decrease opacity and increase accountability in the decision-making process itself.[45]

The Hughes-Ryan Amendment also established a new information-sharing regime between Congress and the executive branch. The statute identified two new committees to which the CIA was to report, "in a timely fashion, a description and scope of such operations": the Senate Committee on Foreign Relations and the House Committee on Foreign Affairs.[46] This reporting requirement was additional to the CIA's prior reporting

---

[39] DYCUS ET AL., *supra* note 23, at 553; Chesney, *supra* note 17, at 588; *see* DONOHUE, *supra* note 38, at 8–9.
[40] DYCUS ET AL., *supra* note 23, at 553.
[41] *Id.* at 507, 552–53; Wall, *supra* note 17, at 104; *see* MICHAEL E. DEVINE, CONG. RSCH. SERV., R45421, CONGRESSIONAL OVERSIGHT OF INTELLIGENCE: BACKGROUND AND SELECTED OPTIONS FOR FURTHER REFORM 3 (2018).
[42] *See* Foreign Assistance Act of 1974, Pub. L. No. 93-559, sec. 32, § 662(a), 88 Stat. 1795, 1804. Notably, at the same time that the Hughes-Ryan Amendment was enacted, the executive also received additional congressional checks on war-making ability through the War Powers Resolution.
[43] *Id.*
[44] Chesney, *supra* note 17, at 588–89.
[45] *Id. See* DEVINE, *supra* note 41, at 2; *see also* MICHAEL E. DEVINE, CONG. RSCH. SERV., R45196, COVERT ACTION AND CLANDESTINE ACTIVITIES OF THE INTELLIGENCE COMMUNITY: FRAMEWORK FOR CONGRESSIONAL OVERSIGHT IN BRIEF 4 (2019) ("Although Congress has no statutory prerogative to veto covert action when informed through a presidential finding, it can influence conduct of an operation through the exercise of congressional constitutional authority and responsibilities to authorize war, legislate, appropriate funds, and otherwise interact with the executive branch.").
[46] Foreign Assistance Act of 1974, sec. 32, § 662(a); Chesney, *supra* note 17, at 589–90.

requirements to the Armed Services Committees and the Appropriations Committees of both Houses.[47] These information-sharing requirements, along with the presidential finding, was Congress's attempt to place meaningful checks on executive authority over covert action that would end an era of "plausible deniability" for the executive.[48]

The Hughes-Ryan Amendment was an extension of the developing legal framework that started a year prior to its enactment with the passage of the 1973 War Powers Resolution (WPR).[49] The WPR was similarly focused on placing a check on the executive's war-making power.[50] At the time, Congress viewed such powers asserted solely by the President as being out of step with the Framers' intent and the necessary balance of powers between Congress and the executive.[51] Yet the WPR did not address covert action; rather, its main focus was to constrain unilateral executive authority over military activity.[52] Similar to the Hughes-Ryan Amendment, the statute created information-sharing and findings requirements. Under the WPR, the President was required to notify Congress within forty-eight hours of any case in which U.S. Armed Forces were "introduced into hostilities or into

---

[47] DYCUS ET AL., *supra* note 23, at 559.

[48] 1 S. REP. NO. 94-755, at 58 (1976); *see also* Chesney, *supra* note 17, at 589–90.

[49] War Powers Resolution, Pub. L. 93-148, 87 Stat. 555 (1973) (codified at 50 U.S.C. §§ 1541–1548). The War Powers Resolution provides that the President can send U.S. Armed Forces into hostilities (or imminent involvement in hostilities) abroad "only pursuant to (1) a declaration of war, (2) specific statutory authorization, or (3) a national emergency created by attack upon the United States, its territories or possessions, or its armed forces." 50 U.S.C. § 1541(c). It also requires the President to notify Congress within forty-eight hours of committing armed forces to military action, among other requirements. § 1543(a).

[50] *See* 50 U.S.C. § 1541.

[51] *See generally* Jack Goldsmith, *The Accountable Presidency*, NEW REPUBLIC (Feb. 1, 2010), https://newrepublic.com/article/72810/the-accountable-presidency (discussing the War Powers Resolution as a congressional reform with some teeth that may have slowed presidential war-making and has at least made the President more accountable to Congress). There is an argument regarding the balance of constitutional powers of the President and Congress with regard to war power. Some argue the authority to initiate war lay with Congress with its authority to declare war and the power of the purse, and that the President may only repel sudden attacks under the authority as Commander-in-Chief and Chief Executive and the authority to conduct foreign relations. *Cf. id.* ("[T]he larger picture is one that preserves the original idea of a balanced constitution with an executive branch that remains legally accountable despite its enormous power."). While the full constitutional background between congressional and presidential powers is outside the scope of this article, it is enough to say that it is predominantly recognized that there must at least be some balance of these powers in war-making.

[52] Chesney, *supra* note 17, at 587; *see* 50 U.S.C. § 1541.

situations where imminent involvement in hostilities is clearly indicated by circumstances; [or] into the territory, airspace or waters of a foreign nation, while equipped for combat . . . ."[53] Congress was also able to terminate such operations within sixty days if it did not authorize them in the interim.[54]

While the Hughes-Ryan Amendment and the WPR began to fill out the legal framework for covert intelligence actions and overt military actions, gaps quickly emerged. Most problematic of these gaps was that both statutory schemes appeared silent about military activity conducted below the threshold of armed conflict. The Hughes-Ryan Amendment had nothing to say about military covert activity and the WPR had nothing to say about persistent low-intensity conflict below the threshold of armed conflict.[55] Further, the WPR only restricted the "Armed Forces" and its members, and was thus silent about covert paramilitary operations conducted by U.S. agents not part of the Armed Forces.[56]

Congress wanted to bring conflict out of the shadows and create more accountability with the enactment of the Hughes-Ryan Amendment and the WPR. In a rather ironic twist, however, the statutes instead created fertile grounds for conducting shadow wars. The creation of these statutory schemes planted the seeds for war-making to go even farther underground or remain covert and below the threshold of armed conflict to "evade congressional notice and control."[57] As a result, the Title 10/Title 50 debate and the blending of authorities put down roots.

Recognizing that more needed to be done, Congress continued to build in oversight and clarify authorities. Less than two years after the enactment of the WPR and Hughes-Ryan Amendment, Congress established two committees to investigate oversight and authorities related to intelligence activities—one chaired by Senator Frank Church in the Senate (the "Church Committee") and the other by Representative Otis Pike in the House (the "Pike Committee").[58] The Church Committee examined at length whether

[53] War Powers Resolution § 4(a)(1)–(2) (codified at 50 U.S.C. § 1543(a)(1)–(2)).
[54] *Id.* § 5(b) (codified at 50 U.S.C. § 1544(b)).
[55] *See* Chesney, *supra* note 17, at 589–90.
[56] DYCUS ET AL., *supra* note 23, at 558.
[57] *Id.*
[58] DEVINE, *supra* note 41.

the United States required secret activities.[59] Both the committee and the executive branch agreed that clear statutory schemes and strong and effective oversight for intelligence agencies were necessary if a permanent secret intelligence system and its activities were to continue.[60] Accordingly, the committee recommended creating the permanent Committees on Intelligence Activities, with the understanding that if the new oversight procedures proved insufficient over time that additional statutory controls could be instituted.[61] Intelligence agencies that conducted secret activities, such as the CIA, would be required to report their activities to the Intelligence Oversight Committees.[62]

In his supplemental statement in the committee report, Senator Charles Mathias, Jr.—an initial proponent of establishing the Church Committee[63]—raised important points that summarized most of the shared sentiment in Congress surrounding secret intelligence activities at the time. Senator Mathias noted that, "in view of dangers involved, and the past record of instances of recklessness harmful to the nation there is a need for more caution through more accountability and fixed responsibility in the decisionmaking process governing the initiation and carrying out of intelligence activities."[64] He considered a thorough and rigorous paper trail essential for such secret activities.[65] Importantly, he concluded, "[t]he possible drawbacks of a monitoring system of extensive checks and balances are far outweighed by the dangers of unchecked secret activities. . . . In a time of peace a rigorously enforced system of checks and accountability is necessary for the preservation of a free society."[66]

Following the implementation of the Church Committee's recommendations, the legal framework continued to grow. The 1980 Intelligence Oversight Act established the recommended congressional Committees on Intelligence Activities and expounded on the Hughes-Ryan Amendment's reporting requirements,[67] directing that the executive branch

---

[59] 1 S. REP. NO. 94-755, at 609 (1976).
[60] *Id.*
[61] *Id.* at 613; *see* DEVINE, *supra* note 45, at 1; DEVINE, *supra* note 41, at 3–4.
[62] *See* 1 S. REP. NO. 94-755, at 470, 611, 613; DEVINE, *supra* note 41, at 4.
[63] 1 S. REP. NO. 94-755, at 609.
[64] *Id.* at 613.
[65] *Id.*
[66] *Id.*
[67] *See* S. 2284, 96th Cong. (1980). The Hughes-Ryan Amendment became outdated with the creation of the Senate and House Select Committees on Intelligence. DEVINE, *supra* note 41,

report any "anticipated intelligence activity" to the committees.[68] The Intelligence Oversight Act's provisions became law through incorporation in the Intelligence Authorization Act for Fiscal Year 1981.[69] Additionally, a series of executive orders attempted to further fill gaps in the legal framework, ultimately culminating in President Regan's iconic Executive Order 12333 of 1981.[70]

Executive Order 12333 further clarified covert action authority and roles among the military and intelligence agencies.[71] At the time of enactment, though, "covert actions" were not clearly defined in any statute and were instead referred to as "special activities."[72] Under this authority, Congress assigned the CIA primary responsibility for special activities, subject to certain stipulations.[73] First, the Armed Forces could use such activities in a time of declared war by Congress or any period of time covered by a report from the President to Congress consistent with the WPR.[74] Second, these activities could be used by another agency if the President determined that the agency would be more likely to achieve a particular objective.[75]

In the mid-1980s, sentiment again grew for more changes to the legal framework as the media exposed what became known as the "Iran-Contra Affair." In 1986, the Intelligence Committees learned that the CIA had secretly laid mines on Nicaraguan waters and provided support to the

---

at 3, n.4. It was further "amended by the Intelligence Authorization Act of 1981 and formally repealed by the Intelligence Authorization Act for Fiscal Year 1991." *Id.*

[68] Intelligence Authorization Act for Fiscal Year 1981, Pub. L. No. 96-450, sec. 407(b)(1), § 501(a)(1), 94 Stat. 1975, 1981 (1980) (codified as amended at 50 U.S.C. § 3092(a)(1)). The act requires U.S. Government agencies to report covert actions to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. *Id.*

[69] *See id.*

[70] *See* Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981), *amended by* Exec. Order No. 13470, 73 Fed. Reg. 45325 (July 30, 2008); *see also* Chesney, *supra* note 17, at 590–92.

[71] *See* Exec. Order No. 12333, 46 Fed. Reg. at 59946.

[72] *Id.* at 59943. Later amendments changed "special activities" to "covert action." Exec. Order No. 13470, 73 Fed. Reg. at 45333.

[73] Exec. Order No. 12333, 46 Fed. Reg. at 59941.

[74] *Id.* at 59946.

[75] *Id. But cf. Questions for the Record: Caroline D. Krass*, U.S. SENATE 1–2, https://www.intelligence.senate.gov/sites/default/files/hearings/krasspost.pdf (last visited Oct. 10, 2021) (noting that this caveat does not give the President complete discretion in determining which agency should carry out covert actions; the statutory definition of covert action must still be considered).

Contras, an insurgent group, against the Sandinista government.[76] Efforts by the CIA included secret arms sales to Iran, through Israel, to be diverted to the Contras in opposition of congressional authorizations.[77] The CIA also assisted the Contras in secret psychological operations, as evidenced by the CIA's composition and distribution of a manual describing "selective use of violence for propagandistic effects" and recommending that the Contras lure demonstrators into clashes with authorities to enflame public sentiment against the government.[78]

The investigation into the Iran-Contra Affair concluded that the scandal was not a direct result of the mounting patchwork of legal controls, but rather a failure to follow existing law.[79] Contrary to explicit statutory requirements, the President failed to notify the Intelligence Committees of the CIA's covert actions and waited two years before informing Congress of other actions.[80] Congress, in response, further clarified covert action authorities and strengthened oversight.

*3. Setting the Stage for the Fifth Fight: Covert Actions and Traditional Military Activities*

After much debate and impasse between the legislative and executive branches over a number of years on how to reform covert action authorities in light of the Iran-Contra Affair, a compromise finally came with the enactment of the Intelligence Authorization Act, Fiscal Year 1991 (1991 Act).[81] Two major developments arose out of this act.[82] First, it created a statutory definition of "covert action," which Congress defined broadly without reference to any particular agency (though the definition on which

---

[76] DYCUS ET AL., *supra* note 23, at 557; *see* S. REP. NO. 100-216 (1988); James S. Van Wagenen, *A Review of Congressional Oversight*, 40 STUD. INTEL. 97, 101 (1997).
[77] DYCUS ET AL., *supra* note 23, at 557.
[78] PSYCHOLOGICAL OPERATIONS IN GUERRILLA WARFARE 10–11 (1984).
[79] DYCUS ET AL., *supra* note 23, at 558; *see* Van Wagenen, *supra* note 76.
[80] *Covert-Disclosure Bill Is Signed by President*, N.Y. TIMES, Aug. 16, 1991, at A11; *see* DEVINE, *supra* note 45, at 5, n.16.
[81] *See, e.g.*, *Covert-Disclosure Bill Is Signed by President*, *supra* note 80; Chesney, *supra* note 17, at 593–98. With the enactment of the Intelligence Authorization Act, Fiscal Year 1991, the Hughes-Ryan Amendment was repealed and portions of the 1991 act were added to the Intelligence Oversight Act of 1980 to clarify the oversight and reporting of intelligence activities and covert actions. *See* Intelligence Authorization Act, Fiscal Year 1991, Pub. L. No. 102-88, §§ 601–603, 105 Stat. 429, 441–45 (codified as amended at 50 U.S.C. §§ 3091–3094).
[82] *See* Chesney, *supra* note 17, at 593–600.

Congress settled closely resembled the one previously set forth by the CIA).[83] The 1991 Act, which controls today, defines covert action as "an activity or activities of the United States Government *to influence* political, economic, or military conditions abroad, where it is intended that the role of the United States Government *will not be apparent or acknowledged publicly*."[84]

The second major development the 1991 Act produced was the recognition that some forms of unacknowledged military action should fall outside the covert action oversight regime.[85] The statute defined those military actions as "traditional military activity" (TMA) or "routine support" to such activities.[86] These military activities were placed among a list of activities that Congress exempted from the covert action oversight and decision-making regime.[87] It was TMA that later became the epicenter for most of the internal Government debate surrounding cyberspace activities or operations—the foundation or impetus for what this article refers to as the fifth fight.

---

[83] *See* Intelligence Authorization Act, Fiscal Year 1991 sec. 602(a)(2), § 503(e) (codified as amended at 50 U.S.C. § 3093); Chesney, *supra* note 17, at 593.

[84] Intelligence Authorization Act, Fiscal Year 1991 sec. 602(a)(2), § 503(e) (codified as amended at 50 U.S.C. § 3093(e)) (emphasis added).

[85] *See id.*

[86] *Id.*; 50 U.S.C. § 3093(e)(2); *see* S. REP. NO. 102-85, at 46 (1991).

[87] 50 U.S.C. § 3093(e)(1)–(4). The full list includes:

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

*Id.* Although some cyber operations might be defined as intelligence collection (thus removing it from the covert action regime), this categorization turns out to be irrelevant insofar as congressional notification is concerned since the NSA requires intelligence collection to be reported to the Intelligence Committees. Robert Chesney, *Computer Network Operations and U.S. Domestic Law: An Overview*, 89 INT'L L. STUD. 218, 220 (2013); *see* 50 U.S.C. § 3092(a).

The concept of TMA has been ripe for debate from its inception.[88] This is mainly because Congress did not define TMA in the 1991 Act or in any statute since. Thus, legislative history is useful to aid in statutory interpretation. Practitioners traditionally look to the Congressional Intelligence Committee reports surrounding the enactment of the 1991 Act for a general definition that Congress had in mind, which was quite narrow.[89]

In its initial report, the Senate Intelligence Committee generally defined TMA as those activities that "encompass 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."[90] The Committee stated its intent to include within the concept of TMA those military operations where the sponsorship of the United States would be apparent or acknowledged at the time of the operation.[91] Such operations included, for example, military contingency operations, rescuing U.S. hostages, accomplishing counterterrorist objectives, supporting counternarcotic operations, or achieving limited military objectives.[92] The Committee report

---

[88] *Cf.* H. REP. 101-725, pt. I (1990) ("[B]ecause of the complexity of the international environment in which our country must act, sometimes discreetly, it is not possible to craft a definition of 'covert action' so precise as to leave absolutely no areas of ambiguity in its potential application.").

[89] *See* Chesney, *supra* note 17, at 595; *see also Questions for the Record: Caroline D. Krass*, *supra* note 75 (relying on legislative history of section 503(e) of the National Security Act, as amended, for "helpful guidance on the meaning of 'traditional military activities'"). There is another viewpoint on how to interpret traditional military activity (TMA), which is a history-based interpretation where an activity is analogous to a historical activity. This type of interpretation, however, becomes precarious in the context of cyber operations that typically have little analogy to prior historical operations. Chesney, *supra* note 87, at 221. For this reason, this article relies on the interpretation of TMA that uses the legislative history as a guide. It is also worth noting that the traditional history-based interpretation fails to recognize that Congress wanted to temper what the Pentagon once thought to be TMA that were unacknowledged. Further, it is long-established practice of the interagency to look at the committee reports for an understanding of TMA. *See, e.g.*, Jeff Mustin & Harvey Rishikof, *Projecting Force in the 21st Century—Legitimacy and the Rule of Law: Title 50, Title 10, Title 18, and Art. 75*, 63 RUTGERS L. REV. 1235, 1237–38 (2011).

[90] S. REP. NO. 101-358, at 54 (1990); S. REP. NO. 102-85, at 46 (1991). Of note, Senate Report 101-358 was the Senate committee report accompanying its initial proposed Intelligence Authorization Act, Fiscal Year 1991, which is virtually identical to the enacted bill but for one sentence in the covert action definition that did not affect the TMA definition. *See* S. REP. NO. 102-85, at 2.

[91] S. REP. NO. 101-358, at 54.

[92] *Id.*

explicitly excluded from the definition of TMA any unacknowledged military activities, with the minor exception of "routine support" activities where the supported or planned military operation was ultimately to be apparent or publicly acknowledged.[93]

Routine support activities were also fairly narrow in scope. The Committee considered these activities to include, for example, providing false documents, currency, or communication devices to persons involved in a military operation that is to be publicly acknowledged.[94] Other routine support could include caching communications equipment or weapons in a target country, leasing property to support future operations, or procuring the storage of vehicles or equipment.[95] Such activities could qualify as routine support only if all such activities were to lead to an operation that, as a whole, would be publicly acknowledged.[96] Moreover, the Intelligence Committee considered unacknowledged operations like "influencing foreign public opinion" or "inducing foreign persons to take certain actions" as posing more serious risks for the United States, concluding that such operations should similarly fall outside the scope of TMA or routine support activities.[97] After carving out TMA and routine support activities, Congress left little wiggle room for any unacknowledged military activities (while leaving no room for unacknowledged military operations) within the definitions of TMA and routine support.

The 1991 Act's broad definition of covert action and narrow definition of TMA, paired with minimal opportunities for the military to conduct unacknowledged and influencing activities, raised serious concerns with senior DoD officials in the Pentagon.[98] These officials became concerned that the definitions and espoused congressional intent would be interpreted as encompassing more activities than those usually defined as covert action, thereby encroaching on TMA that normally did not fall within the covert action oversight regime.[99] Defense officials were especially concerned about "strategic deception operations, certain peacetime psychological

[93] *Id.*
[94] *Id.*
[95] *Id.* at 54–55.
[96] *Id.*
[97] *Id.* at 55.
[98] H.R. REP. NO. 101-725, pt. 1 (1990).
[99] *Id.*

operations, some advance support contingency operations, and certain elements of some counterintelligence operations."[100]

As a compromise between Congress and the executive branch, the Committees slightly broadened the definition of TMA by exempting some additional unacknowledged military activities.[101] The Committees accomplished this by requiring a military activity to meet four elements to be considered TMA under its general definition.[102] The Committees in both Senate and House reports stated that military activities may be considered TMA (i.e., exempted from the covert action framework) if those activities were: (1) conducted by military personnel; (2) under the direction and control of a U.S. military commander; (3) preceding or related to hostilities that are anticipated to involve U.S. military forces or where such hostilities are ongoing; and (4) where the U.S. role in the *overall operation* is apparent or acknowledged publicly.[103] In the end, while giving some leeway to DoD officials, Congress held on to the final requirement that the military operation itself be apparent or publicly acknowledged, even if the activities leading to the operation were to remain unacknowledged.

In their reports, the Committees provided little additional guidance on interpreting the four elements, with the exception of having a military commander. The Committees were clear in drawing a line with regard to TMA, in that it would only include those activities "under the direction and control of the military commander."[104] The Committees offered no qualifying language for this element and specifically stated that those activities not under the direction and control of a military commander should not be considered TMA.[105]

In contrast, the vagueness of the third element of anticipated or ongoing hostilities presents the most challenges for interpretation. To satisfy this element, the Committees required activities (1) to precede or relate to hostilities that are anticipated to involve military forces (meaning approval

---

[100] *Id.*

[101] *See* Chesney, *supra* note 17, at 598–99.

[102] S. REP. NO. 102-85, at 46 (1991); H.R. REP. NO. 102-166, at 30 (1991) (Conf. Rep.).

[103] S. REP. NO. 102-85, at 46. Conferees also noted that it does not matter if the United States' sponsorship of such activities is immediately apparent or later to be acknowledged; the ultimate crux is that in the fourth element is an intent to reveal the United States' involvement in the overall operation. *See id.*

[104] *Id.*; *see* H.R. REP. NO. 102-166, at 29–30.

[105] S. REP. NO. 102-85, at 46; H.R. REP. NO. 102-166, at 30.

has been given by the National Command Authorities (i.e., the President or Secretary of Defense) for the activities and for operational planning for hostilities); or (2) where hostilities are ongoing.[106] The problem is that, given these two options, "anticipated" hostilities could be read broadly. If "anticipated" hostilities meant mere planning for events that could foreseeably result in some military force, it would lend to a reading where unacknowledged military activities could almost always be authorized under this requirement. Such a reading, though, is too broad in light of Congress's previous objections and fairly narrow original conception of TMA and routine support.

To better understand the third element of anticipated or ongoing hostilities, one might first examine those instances where the Committees specifically indicated that this element was not required for qualification under the TMA exception. This means examining what qualifies as the "routine support" activities mentioned above, which effectively eliminates the need for anticipated or ongoing hostilities.[107] In outlining the boundaries of TMA, the Committees recognized that military forces may be required to conduct unacknowledged activities to support the planning and execution of a military operation that was to be acknowledged, should that military operation become necessary even in the absence of the third element requiring anticipated or ongoing hostilities.[108] The Committees classified these activities as "routine support" to TMA, a subset of supporting activities under the TMA exemption.[109]

The Committees were consistent in setting clear limits on what qualified as "routine support," concluding that it would only constitute those *unilateral* U.S. activities that provided or arranged for logistical or other support for U.S. military forces in the event of a military operation that was to be publicly acknowledged.[110] In the final Senate committee report, the Committee again stood by its examples of this "routine support" to include caching communications equipment or weapons, leasing or purchasing from unwitting sources residential or commercial property to support operations,

---

[106] S. REP. NO. 102-85, at 46. The National Command Authority refers to approval by both the President and the Secretary of Defense.
[107] *See* S. REP. NO. 101-358, at 54–55 (1990).
[108] *See id.*
[109] S. REP. NO. 102-85, at 46; *see* 50 U.S.C. §3093(e)(2).
[110] S. REP. NO. 102-85, at 47; *see* H.R. REP. NO. 102-166, at 30 (agreeing with the explanation for routine support as described in the Senate report).

or obtaining currency for possible operational use.[111] Again, all such activities would qualify as "routine support" only so long as the supported operation as a whole was to be publicly acknowledged.[112]

The Committees, however, regarded "other-than-routine" support activities, or those activities not qualifying for the exemption, to be those activities that were not unilateral, such as attempts to recruit or train foreign nationals with access to the target country, clandestine effects to influence foreign nationals to take certain actions in the event of a U.S. military operation, efforts to influence and affect public opinion in the country concerned where U.S. sponsorship of such efforts is concealed, and clandestine efforts to influence foreign officials in third countries to take certain actions without the knowledge or approval of their government in the event of a U.S. military operation.[113] Given this list, according to Congress, key unacknowledged influencing operations were certainty off the table for the military as TMA or routine support. The military's conduct of these "other-than-routine" activities that fell outside anticipated or ongoing hostilities would then constitute covert action, falling under the covert action oversight regime.

Taking into consideration Congress's intended scope of "routine support," if activities do not constitute this "routine support," the element of anticipated or ongoing hostilities must otherwise be met for the TMA exemption to apply. Of course, this leads back to the original question of how broadly "anticipated" hostilities should be interpreted. Professor Robert Chesney offered a possible explanation for how to understand this broad category of anticipated hostilities in 2012, suggesting that anticipated hostilities should be viewed in light of crisis response and limited contingency operations, which are outlined as a category of a range of military operations in the defense joint publication on joint military operations.[114]

Joint Publication 3-0 outlines three primary categories for the range of military operations: (1) military engagement, security cooperation, and deterrence; (2) crisis response and limited contingency operations; and (3)

---

[111] S. REP. NO. 102-85, at 47.
[112] *Id.*
[113] *Id.*; *see* H.R. REP. NO. 102-166, at 30.
[114] *See* Chesney, *supra* note 17, at 599–600.

large-scale combat operations.[115] The range depicts operations conducted in peacetime and those conducted in the context of armed conflict, with a great deal of space in between. Crisis response and limited contingency operations are those operations that might fall somewhere between peace and conflict and are specifically defined in Joint Publication 3-0 as situations that require military operations in response to natural disasters, terrorists, subversives, or other contingencies and crises as directed by the appropriate authority.[116] In military doctrine, these types of operations typically fall just below large-scale combat operations on the conflict continuum that spans from peace to war.[117] The conduct of operations that respond to such crises needs to then "anticipate" future hostilities if such operations were to progress. Following this logic, Professor Chesney's suggestion makes great sense.

Taking Professor Chesney's suggestion a step further means that "anticipated" hostilities would exclude those operations that constitute military engagement, security cooperation, or deterrence—essentially anything below crisis response and limited contingency operations. According to Joint Publication 3-0, these kinds of "activities develop local and regional situational awareness, build networks and relationships with partners, shape the [operating environment], keep day-to-day tensions between nations or groups below the threshold of armed conflict, and maintain U.S. global influence."[118] Essentially, many of these activities falling below crisis response and contingency operations are those that are the main concern and conducted today in countering great power adversaries.

In light of this interpretation, such military activities falling within the category of crisis response and limited contingency operations could still encompass a sweeping range of activities. Professor Chesney notes that Congress recognized this expansion of TMA authority and, in exchange, required a more mild form of decision-making by the National Command Authorities when invoking this authority for unacknowledged military activity.[119] Professor Chesney further claims that, although this was a lesser form of checks on the executive branch than a presidential finding

---

[115] JOINT CHIEFS OF STAFF, JOINT PUB. 3-0, JOINT OPERATIONS, at xvii (17 Jan. 2017) (C1, 22 Oct. 2018) [hereinafter JP 3-0].
[116] *Id.* at xx.
[117] *Id.* at xvii.
[118] *Id.* at V-4.
[119] Chesney, *supra* note 17, at 600; *see* S. REP. NO. 102-85, at 46 (1991).

and information sharing than required for covert action, it nonetheless "mandate[d] a level of internal executive branch authorization that would preclude, for example, a decision by a combatant commander or anyone lower in the chain of command from engaging in an unacknowledged operation other than during times of overt [(or ongoing)] hostilities."[120]

Professor Chesney's forecast of potential restraint on the executive branch and the contours of "anticipated" hostilities is not so obvious today, given the recent enactment of military cyberspace authorities in the NDAA for FY 2019[121] and FY 2020.[122] These NDAA provisions greatly expanded the definition of TMA to include what is essentially all military activities, operations, and preparatory actions in cyberspace—spanning the entire range of military operations. In this sweeping change, Congress went from essentially not allowing unacknowledged military operations (and only allowing a small subset of unacknowledged military activities leading to operations) under the purview of TMA to eliminating altogether this requirement for acknowledging operations in the domain of cyberspace.

The next section examines these developments and how the Title 10/Title 50 debate took the United States into this new realm of TMA and military cyberspace activities and authorities. When Congress redefined the longstanding boundaries of TMA as applied in the evolving domain of cyberspace, the congressional sentiment once surrounding the Church and Pike Committees that called for strong oversight and checks on the executive in conducting secret or covert operations—especially by the military—significantly softened in nuanced ways.[123]

B. The Fifth Domain: Navigating the Legal Framework

*1. The Fifth Domain Challenge and Convergence*

More than any other domain, the domain of cyberspace, known as the "fifth domain," arguably raises the most perplexing legal questions for the

---

[120] Chesney, *supra* note 17, at 600.
[121] National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1632, 132 Stat. 1636, 2123 (2018) (codified at 10 U.S.C. § 394).
[122] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1631(b)–(c), 133 Stat. 1198, 1742 (2019) (codified at 10 U.S.C. § 397 note).
[123] Congressional oversight evidently started to dwindle even before 9/11. *See* DEVINE, *supra* note 45, at 2.

conduct of operations. This is a paradox since, unlike the other domains, cyberspace is man-made and can therefore be changed by man,[124] which makes it the most challenging domain. In their book *The Fifth Domain*, Richard Clarke and Robert Knake summarize this challenging operational environment: "It is a positive attribute of cyberspace that once a weapon has been used and discovered it can be blocked. That is the equivalent of changing the atmosphere so that bombs can no longer fall."[125]

The main challenge of the fifth domain lies in having to address the asymmetric nature of cyberspace operations, with novel cyber effects continuously appearing on the "battlefield" and ever-changing actors, targets, and terrain. Cyberspace military or intelligence operators, therefore, often need to conduct operations at breakneck pace to address these rapid and emerging threats in a fluid and constantly shifting domain.[126] Actions utilized to achieve "cyberspace effects" in this domain tend to look and present like secret intelligence activities in conjunction with military activities.[127] Put differently, cyberspace effects operations tend to converge the need for collection, analysis, exploitation, and attack into one simultaneous operation,[128] and Government agencies most often conduct these operations in secret to avoid direct attribution or allow for quick reaction or offensive surprise.

To complicate matters further, both military organizations, like U.S. Cyber Command, and intelligence agencies, like the NSA, typically conduct cyberspace operations, albeit separated by their authorized missions and authorities (Title 10 versus Title 50),[129] and regularly converge to achieve

---

[124] *See* CLARKE & KNAKE, *supra* note 16, at 6.

[125] *Id.*

[126] *See, e.g.*, U.S. CYBER COMMAND, *supra* note 6, at 2; *cf. Department of Defense's Cybersecurity Acquisition and Practices from the Private Sector: Hearing Before the Subcomm. on Cybersecurity of the S. Comm. on Armed Servs.*, 115th Cong. 3–4 (2018) (statement of Dmitri Alperovitch, Co-Founder & Chief Tech. Officer, CrowdStrike).

[127] *See, e.g.*, Brown & Metcalf, *supra* note 17, at 117 ("[T]he techniques of cyber espionage and cyber attack are often identical, and cyber espionage is usually a necessary prerequisite for cyber attack.").

[128] *See id.*; Wall, *supra* note 17, at 121; *see also* General (Retired) Michael Hayden, *Cutting Cyber Command's Umbilical Cord to the NSA*, CIPHER BRIEF (July 17, 2017), https://www.thecipherbrief.com/cutting-cyber-commands-umbilical-cord-to-the-nsa ("[I]n the cyber domain the technical and operational aspects of defense, espionage, and cyberattack are frankly indistinguishable—they are all the same thing.").

[129] *See* Hayden, *supra* note 128; Emma Kohse & Chris Mirasola, *To Split or Not to Split: The Future of CYBERSOM's Relationship with NSA*, LAWFARE (Apr. 12, 2017, 1:03 PM), https://

full operational success. The dual-hatted role of NSA director and U.S. Cyber Command commander, and the resulting interagency bleed-over, make this no less of a challenge.[130] Yet one of the considerations in originally creating the dual-hat was the very recognition that there was a "high potential of overlap between military and intelligence operations in cyberspace."[131] A dual-hatted commander and director would have the ability to de-conflict and prioritize those competing military and intelligence interests across both organizations to allow cyberspace operations to move smoothly.[132] While some have recently argued for the end of the dual-hat,[133] the need for shared infrastructure, technical resources, expertise, and even authorities arguably makes this complex structure a necessity for sustained defense capabilities and the effective projection of combat power, at least for now.[134]

The challenging nature of cyberspace operations have made it equally challenging to govern these operations within the construct of any existing legal framework, international or domestic. As Harold Koh noted in 2012, one might ask how our existing legal frameworks can take into account or change based on all the novel kinds of effects that can be produced by state and non-state actors in cyberspace.[135] In answering his own question, Koh retorted, "the difficulty of reaching a definitive legal conclusion or consensus among States on when and under what circumstances a hostile cyber action would constitute an armed attack does not automatically

---

www.lawfareblog.com/split-or-not-split-future-cybercoms-relationship-nsa (discussing the NSA's and U.S. Cyber Command's significant technological overlap, but largely different legal authorities to conduct espionage or offensive operations under Title 50 and Title 10, respectively).

[130] *See* Chesney, *supra* note 17, at 607.

[131] *Time to End the Dual Hat?*, COUNCIL ON FOREIGN RELS. (Feb. 3, 2021, 3:23 PM), https://www.cfr.org/blog/time-end-dual-hat; *see also* Michael Sulmeyer, *Much Ado About Nothing? Cyber Command and the NSA*, WAR ON THE ROCKS (July 19, 2017), https://warontherocks.com/2017/07/much-ado-about-nothing-cyber-command-and-the-nsa.

[132] *Time to End the Dual Hat?*, *supra* note 131.

[133] *E.g.*, Robert Chesney, *Ending the "Dual-Hat" Arrangement for NSA and Cyber Command?*, LAWFARE (Dec. 20, 2020, 8:38 AM), https://www.lawfareblog.com/ending-dual-hat-arrangement-nsa-and-cyber-command (discussing arguments raised for and against splitting the dual hat arrangement between NSA and U.S. Cyber Command).

[134] *Cf. id.*; Javed Ali & Adam Maruyama, *Split up NSA and CYBERCOM*, DEF. ONE (Dec. 24, 2020), https://www.defenseone.com/ideas/2020/12/split-nsa-and-cybercom/171033 (arguing reasons to move forward with the split of the two agencies).

[135] *Harold Koh on International Law in Cyberspace*, OPINIO JURIS (Sept. 12, 2019), http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace.

suggest that we need an entirely new legal framework specific to cyberspace."[136] Today, there remains no significant movement on the international or domestic front to create an entirely new legal framework to deal with cyberspace.[137] Instead, as Koh suggests, legal practitioners must attempt to fit—or more aptly, cram—cyberspace operations into existing legal frameworks.[138]

*2. The Title 10/Title 50 Debate and Convergence*

This not-so-ideal legal situation engendered the Title 10/Title 50 debate in cyberspace operations, which formed the crux of the internal Government debate over the fifth fight. Understanding the debate requires, at a minimum, a basic understanding of its prevailing policy, legal, historical, and operational aspects. A deep-seated policy concern that military personnel should not be involved in secret operations (or "go dark" into the world of espionage) forms the foundation of the debate.[139] The idea is that the military should wear the white hat and remain fully accountable to the public.[140] Operating in the "Title 50 realm" of secret intelligence collection and espionage, then, seems to run counter to this central idea about the U.S. military's purpose.

---

[136] *Id.* (quoting Harold Koh, former Legal Adviser of the U.S. State Department).

[137] Note, though, that some States have started to take positions on whether key principles or rules of international law apply in cyberspace. *See, e.g.*, Michael Schmitt, *France's Major Statement on International Law and Cyber: An Assessment*, JUST SEC. (Sept. 16, 2019), https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment. Additionally, there is notable movement in the area of gaining consensus from States on a handful of norms, or "soft law," that might apply and in some cases be unique in the context of cyberspace. *See generally* Rep. of the Grp. of Governmental Experts on Advancing Responsible State Behav. in Cyberspace in the Context of Int'l Sec., U.N. Doc. A/76/135 (July 14, 2021).

[138] *Cf. Hearing to Receive Testimony on Cyber Strategy and Policy Before S. Comm. on Armed Servs.* 115th Cong. 34 (2017) (statement of Matthew C. Waxman, Professor of Law, Columbia Law School) ("This approach to applying by analogy well-established international legal rules . . . to new technologies is not the only reasonable interpretation, but it is sensible and can accommodate a strong cyber strategy.").

[139] Wall, *supra* note 17, at 88, n.6.

[140] *See id.* Paul Wall, former legal advisor for U.S. Special Operations Command Central, also describes other policy concerns for the military's involvement in secret covert operations, such as "rice bowl" fighting (i.e., the jealous guarding of authorities and responsibilities by the agencies)—a policy concern that is still referenced today by the interagency on a number of issues. *Id.* at 88–89.

Determining what statutory scheme will govern a specific situation or activity typically forms the basis of the legal aspect of the Title 10/Title 50 debate. At a macro level, Title 10 simply refers to the portion of the U.S. Code that addresses the DoD, military law, military service (i.e., Army, Navy, Air Force, Reserves) organizations, and military force or operational authorities.[141] Title 50, on the other hand, refers to the portion of in the U.S. Code that addresses (among other various national security issues and war-making authorities) the intelligence community and its authorities,[142] such as organization of the intelligence community, collection and analysis of foreign intelligence, counterintelligence, and espionage activities.[143] These authorities often overlap in complex ways that can trigger underlying policy debates. In practice, the debate between these authorities can become a challenge to national security law practitioners because they need to answer the sometimes-perplexing statutory question of what authority applies to an operation or activity in order to weigh in on its legality.[144]

---

[141] *See generally* 10 U.S.C. §§ 101–18506.

[142] *See generally* 50 U.S.C. §§ 1–4852. Title 50 is an expansive portion of the U.S. Code that addresses not only intelligence activities and the intelligence community but also national security and war-making activities. *See, e.g.*, *id.* §§ 1541–1550, 1601–1651, 401–442b.

[143] *See, e.g.*, *id.* §§ 31–42. What makes an entity part of the intelligence community is its national foreign intelligence and counterintelligence missions (and designation under the National Security Act). *See id.* § 3003. Intelligence personnel in the military services are also a part of the intelligence community and must follow intelligence community directives and oversight; they are also allowed access to intelligence community information. *See id.* This does not mean that all personnel in the military have a similar designation or access; it is only those military personnel charged with being a part of the intelligence elements of the services or serving in the intelligence elements of an intelligence agency with the mission of conducting foreign intelligence or counterintelligence.

[144] After determining what constitutional or statutory authority allows for overall cyberspace operations, the second question most legal practitioners must ask is which statutory scheme governs a specific operation. The first question is normally one regarding a constitutional balance of powers and whether there is sufficient support under Article II or a supporting congressional authorization, such as an Authorization for the Use of Military Force, or other statutory authority to form the legal basis for U.S. operations abroad. Recently, the fiscal year (FY) 2019 National Defense Authorization Act (NDAA) authorized cyber operations against China, Russia, Iran, and North Korea in response to specific concerns, if approved by the National Command Authority. *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, § 1642(a), 132 Stat. 1636, 2132 (2018). While some might argue that this authority serves as a mini-cyber Authorization for the Use of Military Force, it practically does not rise to that level since the activities permitted generally fall below the use of force. *See, e.g.*, Robert Chesney, *The Law of Military Cyber Operations and the New NDAA*, LAWFARE (July 26, 2018, 2:07 PM), https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa. Section 1642(a) of the FY 2019 NDAA is an

For the historical aspect of the debate, it is important to understand that the issue is not new, but that cyberspace operations have merely exacerbated the problem. The debate traces back to the inception of the covert action legal framework.[145] Generally, the covert action legal framework drove the debate because designating an activity to fall within its framework would carry certain consequences that agencies might attempt to avoid. In other words, when the framework was developed, agencies gained an incentive to evade a designation of covert action for an activity that might otherwise qualify under its definition. It became attractive to agencies to avoid the covert action designation since doing so would yield ostensibly lesser forms of accountability and agency responsibility. Agencies could bypass the presidential finding and robust congressional information-sharing requirements with the Intelligence Committees if an unacknowledged activity was found to not be a covert action and could instead be defined under one of the exemptions, such as TMA.[146] This drove the question of whether agencies were leveraging a Title 10 statutory scheme for military operations versus a Title 50 scheme for intelligence operations. Congress expressed concern that the DoD, for example, too often defines operations as "operational preparation" in order to qualify as TMA when such activities more closely resembled intelligence activities, thinking it was an attempt to circumvent the more stringent oversight requirements of the Intelligence Committees as well as a presidential finding.[147]

Real operational concerns in the fight against terrorism throughout the past twenty years have also greatly impacted the debate. Fighting terrorism abroad drove intelligence and military agencies to occasionally use both

---

example of the type of congressional authorization that could allow for overall offensive cyber operations in the first instance, which is taken into consideration before analyzing the specific type of actions, agencies, and funding that would drive a decision on what statutory scheme or legal framework will govern the actual proposed cyber activity or operation (e.g., looking to the covert action legal framework as the governing scheme).

[145] *See generally* Chesney, *supra* note 17, at 539; Wall, *supra* note 17.

[146] Military forces must still report to the Armed Services Committees. The issue is not a complete lack of congressional oversight. Rather, a covert action finding would require additional reporting across multiple congressional committees (e.g., the Intelligence Committees), resulting in overall higher levels of oversight. *See* Wall, *supra* note 17, at 103; Chesney, *supra* note 87, at 219. Said differently, if the military can define an activity as TMA, there is no obligation to keep the Intelligence Committees informed of the activities in question (or go through the lengthy executive oversight process of a presidential finding determination). *See* Chesney, *supra* note 87, at 220.

[147] *See* DEVINE, *supra* note 41, at 2; *see also* H.R. REP. NO. 111-186, at 50 (2009).

authorities in the conduct of their operations.[148] The CIA, for example, used lethal force authorities under Title 10 while still using covert authorities under Title 50 to allow for greater freedom of movement than military forces were afforded under their Title 10 authorities.[149] Similarly, the military also found itself moving between authorities to combat asymmetric threats. One prime example of this convergence of authorities was the Osama bin Laden operation in 2011, which was primarily conducted by military personnel and commanded by a military commander yet carried out under Title 50 authorities by the CIA and labeled a "covert action" by the executive and the Pentagon.[150]

Such operational developments and challenges with authorities eventually led to greater convergence, the concept where the two realms of military and intelligence agencies conducted activities using both Title 10 and Title 50 authorities, sometimes in conjunction with each other.[151] With greater convergence came more misconceptions surrounding Title 10 and Title 50. Understanding these misconceptions is important for understanding the changes in the legal framework governing cyberspace operations today.

First, Title 10 and Title 50 are not mutually exclusive authorities, but they are mutually reinforcing.[152] Intelligence activities authorized under Title 50 can help to facilitate military activities or operations conducted

---

[148] *See generally* Chesney, *supra* note 17, at 553–80.

[149] *See id.* at 539; Mustin & Rishikof, *supra* note 89, at 1235; Brigadier General Joseph B. Berger III, *Covert Action: Title 10, Title 50, and the Chain of Command*, 67 JOINT FORCES Q., Oct. 2012, at 32.

[150] Berger, *supra* note 149; *Questions for the Record: Caroline D. Krass*, *supra* note 75; Mustin & Rishikof, *supra* note 89, at 1235. It is important to note that much of this debate also stems from a misunderstanding regarding associated rules of engagement and authorities that are separately allowed or approved by the Secretary of Defense and President for the military and intelligence agencies. *See* Wall, *supra* note 17, at 93–94. One of the main reasons the Osama Bin Laden raid proceeded under the CIA's Title 50 authorities was that specific agency authorities would allow the CIA to operate in a country not engaged in hostilities. Jen Patja Howell, *The Lawfare Podcast: Covert Action*, LAWFARE (Mar. 17, 2021, 5:01 AM), https://www.lawfareblog.com/lawfare-podcast-covert-action. Title 10 military forces otherwise had no authorities to operate in a country not engaged in hostilities without prior congressional approval under their war-making authorities. *See id.*

[151] *See, e.g.*, Chesney, *supra* note 17, at 579–83. Convergence between these authorities and their interchangeable use by agencies requires an in-depth discussion that is outside the scope of this article.

[152] Wall, *supra* note 17, at 101.

under Title 10 authorities. Personnel may also exercise these authorities simultaneously under the authority of the Secretary of Defense and the command and control of military commanders.[153] Creating a hardline distinction between Title 10 and Title 50 activities, therefore, creates a distinction not supported by the law.[154] The distinction, instead, has more to do with underlying policy concerns, congressional oversight, and power struggles over authority, direction, and control, including most notably the control over intelligence or military activity associated funds.[155]

Second, intelligence agencies do not have a monopoly over Title 50 authorities. The DoD has elements that are considered part of the intelligence community and operate under both Title 50 and Title 10 authorities, such as the intelligence elements of the military services, defense combat support agencies like the NSA, and the National Geospatial-Intelligence Agency.[156] Another way to view these authorities is that Title 10 and Title 50 clarify roles and responsibilities: sections within Title 10 clarify roles and responsibilities within the DoD, while sections within Title 50 clarify roles and responsibilities within the intelligence community. Despite this distinction, both Titles recognize that the Secretary of Defense has roles and responsibilities under each.[157] As a result, intelligence and defense personnel may also have roles and responsibilities under both.

While the intelligence agencies do not have a monopoly over Title 50, they similarly hold no monopoly over covert action.[158] Title 50 squarely addresses unacknowledged military activities intended to influence political, economic, or military conditions abroad through the covert action statute.[159] The covert action provision within Title 50 would not bar military forces from using covert action; rather, it provides a roadmap for how to do so, regardless of agency.[160] While Executive Order 12333 does address intelligence activities, it also leaves the President with the ability to decide

---

[153] *Id.*; *see also supra* note 143.
[154] Wall, *supra* note 17, at 101.
[155] *Id.*; *see also* DYCUS ET AL., *supra* note 23, at 500, 575.
[156] *See* 50 U.S.C. § 3003; Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981), *amended by* Exec. Order No. 13470, 73 Fed. Reg. 45325 (July 30, 2008)
[157] Wall, *supra* note 17, at 100.
[158] *See* Mustin & Rishikof, *supra* note 89, at 1237 (noting that former CIA director John Rizzo made this very point).
[159] *See* 50 U.S.C. § 3093.
[160] *See id.*

whether covert actions can be undertaken by another agency, including the DoD.[161]

An agency's mission and assessment of the threat, therefore, should be the most persistent drivers of the Title 10/Title 50 debate in determining which agency is best poised under all the available authorities and its mission set to conduct covert operations against a specific threat. For example, recall how the NSC originally identified the CIA as the agency with the ability to conduct covert Cold War activities.[162] At the time, the CIA was in the best position to conduct such activities as an agency that was given a human intelligence mission in peacetime.[163] However, missions and threats change over time. Today, U.S. Cyber Command (and its subordinate units)—a military organization—is now potentially in the best position, given its cyberspace operations mission and capabilities. This leads to a discussion of the current challenge of addressing great power competition and the prevailing use of cyberspace operations.

## III. Constructing the Legal Framework for the Fifth Fight and its Implications

### A. Making the Case for Change: Understanding Cyberspace Operations

Cyberspace operations are inherently likely in many cases to trigger both Title 10 and Title 50 authorities. In the context of cyberspace operations, what might be considered a Title 10 cyberspace "attack" operation may necessarily combine what could be considered a Title 50 intelligence exploitation or collection operation.[164] As a result, operations

---

[161] *See* Exec. Order No. 12333, 46 Fed. Reg. at 59945.
[162] *See* 1 S. REP. NO. 94-755, at 490–91 (1976).
[163] *See generally id.*
[164] Wall, *supra* note 17, at 121. Joint Publication 3-12 defines a cyberspace "attack" as "[a]ctions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires." JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS, at GL-4 (8 June 2018) [hereinafter JP 3-12]. A cyberspace exploitation is defined as "[a]ctions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations." *Id.*

could prompt a range of reporting requirements and concerns over mission responsibility, direction, control, and funding.[165]

It would also matter how one defines the scope of cyberspace operations when determining what authorities apply. At their core, cyberspace operations used to counter great power competition are essentially designed to *influence* some conditions abroad or have some type of influencing effect on adversaries in cyberspace. This could potentially trigger the covert action legal framework if those activities were to also be unacknowledged.[166] On a more granular level, though, certain individual effects or enabling efforts that compose those overall operations can range from looking more akin to traditional espionage activities or perhaps merely preparation of the battlefield or routine support in a traditional military sense.[167] Categorizing cyberspace operations might depend on how one views (or precisely who is viewing, such as military versus intelligence personnel) the scope of those operations. Understanding cyberspace operations holistically, therefore, could result in a categorization of those activities or operations as covert action, intelligence operations, TMA, or all of the above.[168]

Further complicating matters was the ever-prominent question of whether covert cyberspace operations (i.e., those operations intended to influence without U.S. Government acknowledgement) could be considered "traditional" activities at all. If considered TMA, they would just fall within the exclusion under the Title 50 covert action legal framework. Such activities, though, were far from "traditional," so the question was well founded. The technology is relatively new and was not contemplated during the original formation of the legal framework. Although activities affecting communication equipment is as old as military operations themselves, cyberspace is an altogether newly recognized domain.[169] Cyberspace spans far more than just communication equipment; it reaches into infrastructure (physical and logical), data, and metadata that is predominately held in private hands, spanning the globe and affecting the daily lives of citizens

---

[165] *See* DEVINE, *supra* note 41, at 2.
[166] *See* 50 U.S.C. § 3093. "Covert action, plainly stated, is the secret exercise of influence." 1 S. REP. NO. 94-755, at 610.
[167] *See* Brown & Metcalf, *supra* note 17, at 116–18.
[168] See *id.*, for further examples.
[169] *See* JOINT CHIEFS OF STAFF, NATIONAL MILITARY STRATEGY OF THE UNITED STATES OF AMERICA 16 (2004); *see also* William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFFS., Sept./Oct. 2010, at 97, 101.

worldwide.[170] Cyberspace is not just another new technology that can easily be reimagined in the traditional physical or kinetic-based framework, like a tank or nuclear weapon. Instead, cyberspace turned these concepts upside down when it created an entirely new domain for human interaction and revolutionized the global information environment.

The ensuing uncertainty surrounding these issues and statutory requirements resulted in the Title 10/Title 50 debate regarding cyberspace operations. This uncertainty surrounding authorities for cyberspace operations was a major factor that led to the agencies calling on Congress to streamline authorities.[171]

A case for a change in authorities became even more compelling in light of the emerging threat of great power competition.[172] Russia's interference in the 2016 presidential election[173] galvanized the need for the reformation of authorities, with its multifaceted, secretive "active measures" campaign that combined both cyberspace and information operations.[174] These threats from Russia have not allayed in recent years.[175] Similarly, the United States faces asymmetric threats from China in cyberspace, as it continues to engage in cyber malicious activity below the threshold of war and prefers to "conduct covert operations to leverage sufficient deniability."[176] These threats from China, too, are likely to increase as Beijing recognizes the rise

---

[170] The military defines cyberspace as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." JP 3-12, *supra* note 164.

[171] *See* H.R. REP. NO. 115-874, at 1049–50 (2018) (Conf. Rep.); *see also* Chesney, *supra* note 17.

[172] *See generally* discussion *supra* Part I.

[173] *See generally* Indictment, United States v. Internet Rsch. Agency LLC, No. 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[174] *See, e.g.*, Amy Zegart & Michael Morell, *Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail*, FOREIGN AFFS., May/June 2019, at 85, 86.

[175] *See, e.g.*, Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019), https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html; Gary Corn, *Coronavirus Disinformation and the Need for States to Shore up International Law*, LAWFARE (Apr. 2, 2020, 12:30 PM), https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law; *see generally* MORRIS ET AL., *supra* note 6.

[176] BRANDON VALERIANO ET AL., CYBER STRATEGY: THE EVOLVING CHARACTER OF POWER AND COERCION 147 (2018).

of strategic competition and the need for active defenses to respond to growing threats in cyberspace.[177]

To address these growing threats from great power competitors and the compounding Title 10/Title 50 debate over the past few years, the military and intelligence communities appealed to Congress for clarification of authorities. Years of interagency deliberations (primarily between the CIA, Pentagon, Department of Justice, and State Department) about the scope of the covert action legal framework left both the military and intelligence communities feeling hamstrung in their cyberspace operations.[178] Likely compounding these interagency frustrations was the then-existing Presidential Policy Directive on cyberspace operations, which "mapped out an elaborate interagency process that must be followed before U.S. use of cyberattacks."[179] National security practitioners increasingly viewed positive authority without multiple layers of oversight and interagency interference as a requirement for cyberspace operations because of the speed and ever-changing nature of technology, techniques, targets and "terrain" in cyberspace.[180]

The Pentagon, in particular, pleaded to Congress. The conference report for the FY 2019 NDAA outlines how Pentagon officials believed themselves limited in the conduct of cyberspace operations due to the perceived ambiguity in the statutory scheme as to whether cyberspace operations, even those short of cyber attacks or a use of force, would qualify

---

[177] *See* CORDESMAN, *supra* note 5; Lyu Jinghua, *What Are China's Cyber Capabilities and Intentions?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Apr. 1, 2019), https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

[178] *See* H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.); *see also* Chesney, *supra* note 17.

[179] Patrick Barry, *The Trump Administration Just Threw out America's Rules for Cyberweapons*, FOREIGN POL'Y (Aug. 21, 2018, 1:35 PM), https://foreignpolicy.com/2018/08/21/the-trump-administration-just-threw-out-americas-rules-for-cyberweapons; *see also* Erica D. Borghard & Shawn W. Lonergan, *What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?*, COUNCIL ON FOREIGN RELS. (Sept. 10, 2018, 10:18 AM), https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations (discussing that critics of reforming Presidential Policy Directive 20 argued that limiting the role of the intelligence community in decision-making about offensive cyber operations could result in prioritizing military operations over intelligence needs).

[180] *See, e.g.*, Zegart & Morell, *supra* note 174, at 89; *see also* H.R. REP. NO. 115-874, at 1049–50.

as TMA or covert actions.[181] As a result, officials claimed they had been limited to "proposing actions that could be conducted overtly on attributable infrastructure without deniability—an operational space that is far too narrow to defend national interests."[182]

### B. Secret Military Cyber Operations: A "New" Framework and Its Implications

Congress found legislation necessary to solve the military cyberspace operations problem through the proposal of section 1632 of the FY 2019 NDAA. In consideration of the proposed legislation, the congressional conferees saw no "logical, legal, or practical reason for allowing extensive clandestine [TMA] in all other operational domains . . . but not in cyberspace."[183] With this affirmation, the conference report accordingly specified "that military activities and operations, or associated preparatory actions, conducted in cyberspace, marked by, held in, or conducted with secrecy," would qualify as TMA.[184] Notably, the report stated that the proposed provision would "clarify that *clandestine* military activities or operations in cyberspace are traditional military activities for the purposes of section 503(e)(2) of the National Security Act of 1974 . . . ."[185] Historically, such clandestine activities were conducted secretly with an intent to attribute (immediately or with delay) the activity to the United States and done without an intent to influence conditions abroad. As the section below shows, Congress slightly altered this understanding of *clandestine* military activities and TMA for cyberspace activities and operations when they enacted the new statutory provision on cyberspace TMA.

Still, according to the conference report, Congress intended to place some limits on TMA, albeit extremely vague and broad ones. Cyberspace TMA must be carried out under one of three conditions:

> (1) as part of a military operation plan approved by the President or the Secretary in anticipation of hostilities or

---

[181] H.R. REP. NO. 115-874, at 1049.
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.* (emphasis added). See discussion *supra* Section II.A, for an overview of the usual understanding of clandestine activities.

> as directed by the President or the Secretary, (2) to deter, safeguard, or defend against attacks or malicious cyber activities against the United States or Department of Defense information, networks, systems, installations, facilities, or other assets, or (3) in support of information related capabilities . . . .[186]

Although this list of cyber TMA is broad, the conference report did provide a word of restraint for the Pentagon and expected continued oversight. The report stated that "[t]he conferees do not intend or expect that this provision will result in the Department's unnecessarily or routinely conducting clandestine cyber attacks, especially those outside of areas in which hostilities are occurring . . . ."[187] The provision was not to be read as any type of authorization for the use of force.[188] Additionally, Congress expected "rigorous oversight" of the DoD to continue through the Armed Services Committees.[189]

Though it warned against an indiscriminate use of force or cyberspace attacks, Congress did little more to temper the use of cyberspace TMA to merely deter or support information-related capabilities—two permissible uses of secret cyberspace TMA that span a vast array of cyberspace activities. In fact, Congress specifically urged the military to "pursue more active engagement with and deterrence of adversaries in cyberspace."[190] Heeding the Pentagon's pleas, Congress opened the gates for permissible secret (including unacknowledged) cyberspace activities and operations, categorizing them as TMA that could span the entire range of military operations. Congress intended to expand TMA in cyberspace with minimal restraints and did so by crafting the legislation as an "affirmation" of authority. The hope was that this would give the Pentagon the freedom of movement to "pursue more active engagement with and deterrence of

---

[186] H.R. REP. NO. 115-874, at 1049. "Such activities include those conducted for the purpose of preparation of the environment, force protection, deterrence of hostilities, advancing counterterrorism operations, and in support of information operations or information-related capabilities. Information-related capabilities may include, when appropriate and approved, military deception and psychological operations." *Id.*
[187] *Id.* at 1049–50.
[188] *Id.* at 1049.
[189] *Id.* at 1050.
[190] *Id.*

adversaries in cyberspace" and put an end to any questions about the military's authority to act in this domain.[191]

In August 2018, Congress enacted section 1632 of the FY 2019 NDAA, which was later codified at 10 U.S.C. § 394. Rather than a new grant of authority, most scholars and practitioners view this affirmation of cyber authority as a mere clarification of authorities to end the Title 10/Title 50 debate in cyberspace operations.[192] Considering that Congress specifically styled this section as an "affirmation," this interpretation is logical and seemingly suits congressional intent. However, as indicated above with the scope and categorization of cyberspace operations, such a reading may miss some of the more nuanced practical implications of this clarification. The following sections detail considerations for why this affirmation establishes a new framework for activities and operations conducted by the military in cyberspace and how that framework has implications for the future of great power competition. At the very least, national security practitioners and policymakers should consider these implications going forward.

*1. Quasi-Restraints Lifted*

The covert action legal framework requires more stringent presidential findings and information sharing with Congress. When previously interpreted by the military and intelligence agencies in the context of cyberspace, this framework served as a quasi-restraint on activities and operations, especially by the military. Even though the CIA did not have a monopoly over covert action, the military rarely sought and received the required written finding to conduct covert actions for all the reasons that drove the Title 10/Title 50 debate.[193] In the FY 2019 NDAA House conference report, Congress recognized the DoD's perceived limitations that resulted in proposing military cyberspace operations conducted outside of active hostilities to only include those activities conducted "overtly on attributable infrastructure without deniability" because of the Department's concern for tripping into the covert action framework.[194] Section 394 vastly changed this dynamic, though, by opening the floodgates to secret military cyberspace operations.

---

[191] *Id.*
[192] *See, e.g.*, Chesney, *supra* note 17.
[193] Mustin & Rishikof, *supra* note 89, at 1237.
[194] H.R. REP. NO. 115-874, at 1049.

To argue whether the authority for clandestine cyberspace operations has always existed and is a mere "affirmation" becomes irrelevant when the practical implication is that the military did not conduct cyberspace operations in this manner before the enactment of Section 394. Business is no longer business as usual. Secret cyberspace operations now have the ability to more easily become an acceptable norm by the military under this affirmation. This was not an obvious interpretation of TMA prior to Section 394, especially given the congressional history of the covert action legal framework and previous understanding of the TMA exemption.

*2. Clandestine is Covert in Cyberspace—The Military "Goes Dark"*

Congress noted that it wanted to clarify *clandestine* military activity for cyberspace operations; however, it ended up defining the term "clandestine" in this context as having the same meaning as the term "covert."[195] Congress defined "clandestine military activity or operations in cyberspace" to mean those military activities (authorized by the President or Secretary) in cyberspace or associated preparatory actions that are "marked by, held in, or conducted with secrecy, *where the intent is that the activity or operation will not be apparent or acknowledged publicly* . . . ."[196] Such a definition matches the traditional definition of "covert" in that the United States' involvement is unacknowledged.[197] The crux of that definition is an intent for the operation to remain plausibly deniable.[198] Defining cyberspace TMA in this manner is in stark contrast to the traditional definition of TMA. Recall that Congress was explicit in excluding any unacknowledged military activities from the traditional definition of TMA, with the minor exception of "routine support" activities where the supported or planned military operation was ultimately to be apparent or publicly acknowledged.[199]

Congress's definition also allows all military cyberspace operations or activities and *associated preparatory actions* to fall within this new cyberspace exception of TMA. Expanding the TMA definition for cyberspace in this manner leaves very little foreseeable military cyberspace operations or activities that would remain classified as an intelligence

---

[195] *Compare* 10 U.S.C. § 394(f)(1)(A) (defining "clandestine"), *with* 50 U.S.C. § 3093(e) (defining "covert").
[196] 10 U.S.C. § 394(f)(1)(A) (emphasis added).
[197] *Cf.* 50 U.S.C. § 3093(e).
[198] *Cf. id.*; 1 S. REP. NO. 94-755, at 475 (1976).
[199] S. REP. NO. 101-358, at 54 (1990); *see* discussion *supra* Section II.A.3.

activity supporting operations or covert action, which would have required the additional reporting to the Intelligence Committees.[200] Moreover, the type of activities that Congress laid out as constituting those "clandestine" activities in cyberspace is so sweeping that such a list also does little practical work in limiting this definition.[201]

A cyberspace military activity, therefore, can now look like a covert action in practice while falling under the rubric of "clandestine" TMA. As a result, such activities are removed from the covert action legal framework. According to Section 394, any "clandestine military activity or operation in cyberspace shall be considered a traditional military activity. . . ."[202] In light of this circular statutory reading, where "clandestine" is defined as "covert" and "clandestine" means "TMA," it logically follows that covert cyberspace activities are TMA. To highlight this similarity between covert and clandestine and to avoid confusion, the remainder of the article simply refers to these newly "affirmed" clandestine TMA cyber operations as "secret" (unacknowledged or otherwise) military cyberspace operations.

Nevertheless, one critical and practical difference that remains is that the definition of TMA would still require such activities to be carried out by a military commander. Put differently, the authority now permits all covert (as that term had been previously defined and understood in law) cyberspace operations conducted by military forces under a military command (e.g., U.S. Cyber Command) to be exempted from the covert action legal framework. Since permissible cyberspace TMA spans nearly the entire range of military operations and is no longer limited by an "anticipated" hostilities element,[203] the only true distinguishing feature

---

[200] Even outside of the context of covert action reporting, pursuant to 50 U.S.C. § 3092, all Government agencies conducting "intelligence activities" must keep the Intelligence Committees fully and currently informed of such activities (other than covert action, which would be reported pursuant to Section 3093(b)). Therefore, by Congress's definition of all military cyberspace operations or activities and associated preparatory actions as TMA, those intelligence collection efforts that are in preparation or part of military cyberspace activities and operations no longer have to be reported to the Intelligence Committees as "intelligence activities" if carried out by the military and under military authorities.

[201] *See* 10 U.S.C. § 394(f)(1)(B).

[202] *Id.* § 394(c).

[203] *Cf. id.* § 394; H.R. REP. NO. 115-874, at 1049–50 (2018) (Conf. Rep.); discussion *supra* Section II.A.3; discussion *infra* Section III.B.3.

between covert action and clandestine cyberspace activities that qualify as TMA remains a military commander.

With the only distinguishing element being a military commander for secret cyberspace activities that can be exempted from the covert action statute while influencing activities abroad, the preference for conducting secret activities in cyberspace is effectively shifted to the military. Practically, operations will predominately shift to U.S. Cyber Command (and those cyber units under its direction and control),[204] which is led by a military commander—one who is currently dual-hatted as the director of an intelligence agency, nonetheless. Shifting agency preference matters, though; it once again puts into question the primary policy concern regarding the military conducting covert activities in the first place.[205]

The U.S. Government, therefore, must carefully evaluate whether this "new" authority improperly leverages the military's popularity within society to shield these secret operations from public scrutiny, especially if such activities are those that more closely mirror covert intelligence-type activities.[206] History demonstrates that the American public is uncomfortable with such activities without increased oversight.[207] Practitioners and policymakers need to ask the question about whether the military in some cases truly is the proper organization or agency to lead certain efforts, even though military authorities may permit such activities

[204] *See* 10 U.S.C. § 167b (defining scope of U.S. Cyber Command's authority, direction, and control over cyber forces).
[205] *See, e.g.*, Wall, *supra* note 17, at 88, n.6.
[206] *Cf. id.*; *Confidence in Institutions*, GALLUP, https://news.gallup.com/poll/1597/confidence-institutions.aspx (depicting that approximately 72% of Americans have a great deal or quite a lot of confidence in the military, ranking consistently highest—almost double—among institutions over the years) (last visited Sept. 30, 2021); Megan Brenan, *Amid Pandemic, Confidence in Key U.S. Institutions Surges*, GALLUP (Aug. 12, 2020), https://news.gallup.com/poll/317135/amid-pandemic-confidence-key-institutions-surges.aspx. In 2021, General (Retired) Martin Dempsey, former Chairman of the Joint Chiefs of Staff, spoke at a conference regarding military popularity and trust. There, he questioned whether waiving a bar for the prior military service of the current sitting Secretary of Defense, General (Retired) Lloyd Austin, might be perceived or used to leverage the military's popularity and trust with Americans—something he proposed as a consideration of which to be cautious moving forward. Duke University School of Law, *LENS 2021 | Current Issues in Civil-Military Relations*, YOUTUBE (Mar. 5, 2021), https://youtu.be/uV7HoAS2Ipk.
[207] *See* discussion *supra* Section II.A.2.

or even make it easier—with less statutory and oversight roadblocks—to accomplish such activities.

*3. Eliminating Overt Hostilities and Public Acknowledgment Requirements*

Prior to the enactment of 10 U.S.C. § 394, a determination of whether a particular military activity constituted TMA required that the operation take place in a context of "anticipated or ongoing hostilities" and "where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly."[208] Section 394 wrote these elements out of the statutory framework for secret military cyberspace operations that constitute TMA. There is no longer any mention in the statute or legislative history that secret military cyberspace operations must take place in the context of anticipated or ongoing hostilities or where the *overall* operation is overt or is intended to be overt at some future time.

Section 394(b), instead, clearly provides for secret military cyberspace activities or operations to include operations "short of hostilities" and operations "in areas in which hostilities are *not* occurring," including mere "preparation of the environment" or "information operations."[209] When juxtaposed with the requirements for those traditional or historical TMA, Section 394's broad sweep of permissible unacknowledged military cyber activities is in sharp contrast. Section 394 no longer carries with its TMA definition a requirement for cyberspace TMA to take place in a context of either ongoing or anticipated overt hostilities.[210] Reading the prior definition of TMA in the old Intelligence Committee reports and the new one laid out for cyberspace operations in Section 394 as mutually reinforcing would be incongruous to congressional intent, since they are clearly antithetical provisions. The new provision plainly states that secret military cyber

[208] S. REP. NO. 102-85, at 46 (1991).
[209] 10 U.S.C. § 394(b) (emphasis added).
[210] As discussed in Section II.A.3, the traditional fourth element for TMA requires unacknowledged military activities take place in the context of overt hostilities that are either (1) preceding anticipated hostilities (triggering at least a lesser form of decision-making by either the President or Secretary for the activities or their operational planning) or (2) ongoing. S. REP. NO. 102-85, at 46. *Cf.* Chesney, *supra* note 17, at 603 ("The [traditional] TMA definition does not refer to any hostilities, but specifically to *overt* hostilities.").

operations are TMA for the Title 50 exemption, and no further analysis regarding overt hostilities—anticipated, current, or future—is required.[211]

Secret military cyber operations are now permissible outside of an overall overt operation and can even be conducted in areas in which hostilities are not ongoing. To be sure, the Pentagon and Congress believed these types of operations were squarely the types required for the United States to compete in great power competition.[212] Section 394 is essentially the U.S. Government's attempt to close a gap or seam in the legal framework for cyberspace operations that exposed the Nation to emerging threats in cyberspace. In other words, the United States needed the flexible legal maneuver space to match the shifting strategic and operational environment.

An example of this new authority in action is U.S. Cyber Command's persistent engagement doctrine and "defend forward" strategy.[213] Part of that strategy includes "hunt forward" cyberspace operations that deploy defensive cyber teams around the world at the invitation of allies and partners to look for adversaries' malicious cyber activity on allied and partner networks.[214] Depending on one's perspective, these operations may look like intelligence collection, or perhaps operational preparation of the battlefield, since teams "send insights back from these missions" to enable

---

[211] *See* 10 U.S.C. § 394(b)–(c). Of course, activities must still fall within the actual definition of clandestine (covert) cyber military operations, meaning that they would still have to qualify under one of the three broad categories of clandestine cyber operations. *Id.* § 394(f). Under the TMA definition in the 1991 congressional conference reports, even traditional unacknowledged operational preparation of the battlefield would require a determination that those activities would take place in a context in which overt hostilities were anticipated. S. REP. NO. 102-85, at 46 (1991); H.R. REP. NO. 102-166, at 30 (1991) (Conf. Rep.).

[212] *See* H.R. REP. NO. 115-874, at 1049–50 (2018) (Conf. Rep.).

[213] *See generally* DOD CYBER STRATEGY SUMMARY, *supra* note 8 (discussing persistent engagement and defending forward as an overall DoD cyber strategy to counter malicious cyberspace activities in great power competition, including activity that falls below the threshold of armed conflict); General Paul M. Nakasone & Michael Sulmeyer, *How to Compete in Cyberspace*: *Cyber Command's New Approach*, FOREIGN AFFS. (Aug. 25, 2020), https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity (discussing implementation of the "defend forward" strategy through the doctrine of persistent engagement).

[214] *DOD Has Enduring Role in Election Defense*, U.S. DEP'T OF DEF. (Feb. 10, 2020), https://www.defense.gov/Explore/News/Article/Article/2078716/dod-has-enduring-role-in-election-defense; *see* Julian E. Barnes, *U.S. Cyber Command Expands Operations to Hunt Hackers From Russia, Iran and China*, N.Y. TIMES (Nov. 2, 2020), https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html.

follow-on missions.[215] In most cases, though, these operations do not take place in areas of ongoing or anticipated hostilities, nor do they fit into the category of *unilateral* "routine support," if the activities were ever to be unacknowledged.[216] These operations also fit more appropriately in the category of military engagement or security cooperation.[217] Considering all these factors and the scope of such operations, "hunt forward" operations would not normally trigger consideration as covert action; however, it is the other operations facilitated by "hunt forward" that would be a concern absent Section 394.

As stated above, "hunt forward" operations drive other operations that are part of the persistent engagement doctrine or "defend forward" cyber strategy.[218] That overall doctrine and strategy involves the United States going into foreign "red space" to counter adversarial actions in cyberspace that may have been discovered though activities such as "hunt forward."[219] One can assume that these activities in "red space" will be unacknowledged and outside of areas of open or anticipated hostilities when purposefully conducting operations below the threshold of armed conflict to counter malicious activities and great power competitors.[220] In fact, it is these activities and operations that are truly facilitated by Section 394's "new" authority. When considering the full range of military cyberspace operations and activities that might make up the persistent engagement doctrine or "defend forward" strategy, one can see how prior conceptions about categorizing traditional military or covert operations seem to not hold up well in cyberspace for countering threats in today's strategic environment. Hence, Section 394 aimed to close that gap.

---

[215] *DOD Has Enduring Role in Election Defense*, *supra* note 214; *see* Nakasone & Sulmeyer, *supra* note 213.
[216] *See* 50 U.S.C. § 3093(e)(2); S. REP. NO. 102-85, at 47; *see* H.R. REP. NO. 102-166, at 30.
[217] *See* JP 3-0, *supra* note 115, at xvii.
[218] *See DOD Has Enduring Role in Election Defense*, *supra* note 214; Barnes, *supra* note 214.
[219] Barnes, *supra* note 214. "After getting close to foreign adversaries' own networks, Cyber Command can then get inside to identify and potentially neutralize attacks on the United States." *Id.* According to General Charles Moore, Deputy Commander of U.S. Cyber Command, this means that U.S. Cyber Command "want[s] to find the bad guys in red space, in their own operating environment. . . [in order to] take down the archer rather than dodge the arrows." *Id.*
[220] *Cf. id.*; DOD CYBER STRATEGY SUMMARY, *supra* note 8.

The next question to ask, however, is how far such activities or operations may go—to what end or limitations, if any? What will be the result of closing this gap in the framework? Is the Nation exposing other gaps or seams in the legal framework elsewhere? The only tempering language in this "new" authority comes from the congressional conference report that merely cautions the DoD against any "unnecessary" or "routine" clandestine cyber attacks "outside of areas in which hostilities are occurring,"[221] a restraint that is minimal at best.

A key consideration for restraint is that combining increased secret military cyberspace operations that need not be a part of overt hostilities may create a norm of conducting cyberspace operations where the public and greater portions of Congress have little oversight or insight. With the enactment of Section 394, sentiments of caution, restraint, and rigorous accountability for secret operations once touted by a Church Committee-era Congress receded dramatically in the cyberspace domain. Congress has given the green light for military cyberspace operations to "go dark." Some might argue that this is merely an acknowledgment of how States conduct these types of operations. Nevertheless, America should proceed with caution.

Potentially standing to be lost by blindly accepting the notion that cyberspace operations should be conducted by the military in secret and outside of hostilities is a vast degree of important public acknowledgement and attribution for cyberspace operations, both domestically and internationally. The military previously viewed public acknowledgement of cyberspace operations, for example, as a requirement given the prior interagency understanding of the covert action legal framework.[222] This understanding was likely a significant factor weighing in favor of U.S. Government acknowledgment in the 2018 U.S. cyberspace operations against Russian election interference that became publicized.[223] Publicizing such activities informs Americans about their information environment and what threats they face and how their Government is working to counter them. Without a careful balancing of authorities and policy, public knowledge of what is afoot in cyberspace may become a relic of the past.

---

[221] H.R. REP. NO. 115-874, at 1049–50 (2018) (Conf. Rep.).
[222] *See id.*; *see also* Chesney, *supra* note 17.
[223] *See generally* Nakashima, *supra* note 175 (showing public Government acknowledgement of the U.S. cyber operations against Russian 2018 election interference).

Government policies must consider the implications of these changes in the law and the history of Congress's and the public's contempt for secret Government activities.

More importantly, closing one gap in the legal framework as it applies to secret cyberspace activities may be shortsighted if not carefully balanced with public accountability or other legislative efforts that create a shared responsibility for countering malicious cyber activities. By closing the gap in the legal framework for secret cyberspace operations, thereby allowing for more flexible responses to match the velocity and virality of cyberspace operations abroad, the United States may be exposing and creating an even more precarious gap in the domestic legal framework that supports public-private cybersecurity information sharing and cooperation on domestic infrastructure.

The primary concern here is that using the military in ways that potentially threatens or garners suspicion about threatening civil liberties and America's social fabric—including the military's traditional accountability to the public—could risk damaging Americans' trust in the military.[224] Safeguarding this trust historically drove advocates of military transparency and the DoD's reluctance to have the Nation's Service members "go dark," wanting to ensure the military's reputation remained "untarnished by association with the shadowy world of espionage."[225] But damaging this trust now could have even greater consequences. It will almost certainly hurt efforts to build much needed public-private cooperation for threat sharing and defensive measures on domestic cyber infrastructure—a vital aspect to defending the Nation in an interconnected world. In most cases, major cyber attacks and malicious activities target those private systems and networks, ultimately causing cascading national and global effects.[226] With the recent SolarWinds attack in the United

---

[224] *Cf.* Neil Snyder, *Will the Pandemic Affect America's Confidence in the Military?*, WAR ON THE ROCKS (Apr. 29, 2020), https://warontherocks.com/2020/04/will-the-pandemic-affect-americas-confidence-in-the-military (stating that the "the military enjoys a rare place in American life").

[225] Wall, *supra* note 17, at 88 & nn.2, 6. Admiral Vern Clark, former Chief of Naval Operations of the U.S. Navy, once noted that the line that exists between covert and overt is part of the military's good standing in the world and that America has traditionally been careful to keep the military out of the covert world. *Id.*; *see also Legislation Panel: Discussion & Commentary*, 21 REGENT U.L. REV. 331, 347 (2009).

[226] Examples of such cyber attacks include Sony, NotPetya, WannaCry, and, most recently, SolarWinds. *See, e.g.*, CATHERINE A. THEOHARY, CONG. RSCH. SERV., R45142, INFORMATION

States, this concern should become even more acute for America and potentially show that secret operations abroad are not the ultimate solution.[227]

While some scholars argue that Americans' trust in their military is durable,[228] secret military operations in cyberspace and across the internet (and globally interconnected networks that have the potential to affect the daily lives of all Americans or citizens worldwide) is untested territory. What has been tested and well understood, however, is Americans' outrage over unaccountable secret operations that bleed into the homeland,[229] as well as domestic surveillance and data collection over the internet and telecommunication networks.[230] All of these historical efforts left the

---

WARFARE: ISSUES FOR CONGRESS 7 (2018) (noting the unique nature of the Sony attack, to include "threats of physical destruction, affect[ing] the decisionmaking process of a private company, exploited the human element of fear in a civilian population, imposed extra-territorial censorship, and triggered a response from the U.S. government."); Andy Greenburg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world; Bruce Schneier, *Why the NSA Makes Us More Vulnerable to Cyberattacks: The Lessons of WannaCry*, FOREIGN AFFS. (May 30, 2017), https://www.foreignaffairs.com/articles/2017-05-30/why-nsa-makes-us-more-vulnerable-cyberattacks; Raphael Satter, *IT Company SolarWinds Says It May Have Been Hit in 'Highly Sophisticated' Hack*, REUTERS (Dec. 13, 2020, 6:35 PM), https://www.reuters.com/article/us-usa-solarwinds-cyber/it-company-solarwinds-says-it-may-have-been-hit-in-highly-sophisticated-hack-idUSKBN28N0Y7 (detailing the initial report of the SolarWinds attack by a presumed nation-state attacker); Christopher Bing, *Suspected Russian Hackers Spied on U.S. Treasury Emails—Sources*, REUTERS (Dec. 13, 2020, 1:56 PM), https://www.reuters.com/article/uk-usa-cyber-treasury-exclusive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PI (detailing the initial target of the attack as the private sector supply chain that provided U.S. Government software).

[227] *See* Satter, *supra* note 226; Benjamin Jensen et al., *The Strategic Implications of SolarWinds*, LAWFARE (Dec. 18, 2020, 10:23 AM), https://www.lawfareblog.com/strategic-implications-solarwinds; *see also* Richard J. Harknett, *SolarWinds: The Need for Persistent Engagement*, LAWFARE (Dec. 23, 2020, 4:41 PM), https://www.lawfareblog.com/solarwinds-need-persistent-engagement.

[228] Snyder, *supra* note 224; *see* David T. Burbach, *Gaining Trust While Losing Wars: Confidence in the U.S. Military After Iraq and Afghanistan*, 61 ORBIS 154 (2017).

[229] *See* discussion *supra* Section II.A.2.

[230] *See, e.g.*, DONOHUE, *supra* note 38, at 36–38 (discussing the Edward Snowden leaks that exposed the NSA's questionable domestic surveillance of U.S. persons). It is notable that intelligence agencies, rather than the military, were at the helm of such operations in the past, though it is true that small entities of the U.S. Army were tangentially involved with intelligence agencies in charge of the collection of foreign intelligence and information on U.S. citizens prior to the Church and Pike Committees. *See id.* at 8.

American public and private institutions more cautious of the Federal Government's activities within cyberspace.[231] Hence, lawmakers, policymakers, and practitioners alike need to consider the implications of moving the military into the secret "dark" world of cyberspace activities. In particular, they need to look at the effect such operations will have on efforts to build and strengthen the legal framework and relationships that protect America's domestic infrastructure with public-private partnerships—a framework and relationships that must be built on trust and confidence.

*4. Diluting Executive Checks (and Increasing Operations)*

Section 394 effectively creates an even more diluted structure for checks on the executive branch that is now unique to the cyberspace domain. The prior understanding of the form of checks on the executive branch for secret activities was one that was colored by a presumption that "[t]he possible drawbacks of a monitoring system of extensive checks and balances are far outweighed by the dangers of unchecked secret activities. . . . [and such a system is] necessary for the preservation of a free society."[232] Now, the "affirmation" of authority in Section 394 expands the breadth of allowable military secret cyber operations, an expanse of activities that the executive can "check" by rather permissible and fluctuating internal controls and altogether avoid the prospects of any overt hostilities for awareness to the public. Such a change in practice, one designed specifically for the cyber realm of military activities, challenges whether America is still willing to follow the notion of extensive checks and balances for secret activities.

---

[231] *Cf.* A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RSCH. CTR. (June 4, 2018), https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks; Ewen MacAskill & Alex Hern, *Edward Snowden: 'The People Are Still Powerless, But Now They're Aware'*, GUARDIAN (June 4, 2018, 1:00 PM), https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware (noting how private companies had to respond to Americans' privacy concerns after revelations of Government surveillance); George Gao, *What Americans Think About NSA Surveillance, National Security and Privacy*, PEW RSCH. CTR. (May 29, 2015), https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy (noting how a majority of Americans disapproved of the NSA's bulk data collection and have changed their behavior because of it).

[232] 1 S. REP. NO. 94-755, at 613 (1976).

Before Congress enacted Section 394, all unacknowledged TMA operations undertaken in anticipation of hostilities in the context of an overall overt operation had an additional, albeit more mild, decision-making requirement by either the President or the Secretary of Defense. As Professor Chesney posited in 2012, this lesser form of checks still mandated a level of internal executive branch authorization that would preclude lower-level decision-makers from engaging in an unacknowledged operation other than during times of overt hostilities.[233] While Section 394 defines clandestine military cyberspace activities as those being authorized by the President or Secretary,[234] there are still other considerations that appear to weaken this already "milder form of decision-making"[235] that raise questions about how restrained lower-level decision-makers will actually become in cyberspace.

The FY 2019 NDAA conference report describes covert cyberspace operations occurring "short of hostilities" or in "areas in which hostilities are not occurring" when they are part of a military operation plan approved by the President or Secretary in anticipation of hostilities or as directed by the President or Secretary.[236] While this requirement in the conference report looks similar to the previous TMA requirement for operations conducted in anticipation of hostilities, it is not the end of the analysis. Additional considerations dilute this remaining executive check in the new TMA "affirmation."

First, the language in the new statute and report do not require an overall overt operation as it did before. Second, the provision allows for mere direction by the President or Secretary without mandating that an operation be a part of an operation plan, which could—if agency policies permits—evade the possibility that an operation plan might serve to bring an operation within the context of an overall overt operation. Even still, requiring operations to fall under designated operations plans does not necessarily mean that there will ever be overt operations in that specific operational context. Third, after the enactment of the FY 2019 NDAA, a presidential memorandum revised the process by which cyber operations are vetted and approved, leaving the decision with the Secretary, even if other

[233] *See* Chesney, *supra* note 17, at 600.
[234] 10 U.S.C. § 394(f)(1)(a).
[235] Chesney, *supra* note 17, at 600.
[236] H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.).

agencies object.[237] This presidential action coincided with the withdrawal of Presidential Policy Directive 20, an Obama administration-era process that placed higher level checks on the executive branch.[238] These policy changes were meant to enhance the flexibility of the military (i.e., U.S. Cyber Command), giving more latitude for military cyberspace operations to develop and respond to threats. Consequently, although intentionally, these actions will reduce executive checks and permit far more cyberspace operations than ever before.[239]

Finally, the additional permissible secret cyber operations—beyond those conducted in the context of anticipated hostilities that required an approved military plan—tend to permit an extremely broad range of operations, even more so than before. Significantly, Section 394 allows for such operations outside of anticipated or ongoing activities to be carried out "in support of information related capabilities."[240] With this particular

---

[237] Ellen Nakashima, *U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election*, WASH. POST (Dec. 25, 2019), https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

[238] *See* Robert Chesney, *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*, LAWFARE (Sept. 25, 2018, 6:45 PM), https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes; Robert Chesney, *The Law of Military Cyber Operations and the New NDAA*, LAWFARE (July 26, 2018, 2:07 PM), https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa; Eric Geller, *Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand*, POLITICO (Aug. 16, 2018, 2:39 PM) https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095; Dustin Volz, *Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive*, WALL ST. J. (Aug. 15, 2018, 11:36 PM), https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721.

[239] Nakashima, *supra* note 237; Mark Pomerleau, *New Authorities Mean Lots of New Missions at Cyber Command*, FIFTH DOMAIN (May 8, 2019), https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command (adding how the new decision-making process contributed to far more cyber operations in the months following than ever before); *see* Ellen Nakashima, *White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries*, WASH. POST (Sept. 20, 2018), https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html; *see also National Security Presidential Memoranda [NSPMs]: Donald J. Trump Administration*, FED'N OF AM. SCIENTISTS, https://fas.org/irp/offdocs/nspm/index.html (listing National Security Presidential Memoranda 13 as an offensive cyber operations directive, the contents of which are classified).

[240] 10 U.S.C. § 394(f)(B)(iii).

addition to the authority, one can no longer argue that Congress intended to constrain the President or Secretary to conduct secret operations within the context of crisis response and limited contingency operations, which Professor Chesney once noted as the limits for TMA under the "anticipated hostilities" category.[241]

Rather, this additional category of permissible secret cyberspace operations essentially shifts secret cyberspace operations further left on the conflict continuum into deterrence at a minimum, which rests more in the zone of peacetime than wartime.[242] Cyberspace operations not only have the green light to "go dark" as covert operations but are also now permissible as defensive activity taking place "in the context of 'day-to-day great power competition' rather than in crisis."[243] The strategic environment, with secret cyberspace operations taking place in peacetime, seems to more closely resemble those pre-Church Committee days that prompted the extensive checks on secret activities in the first place. Despite this striking resemblance, Congress seems to have gone the opposite direction in required oversight and executive checks when it comes to the fifth domain of cyberspace. So, perhaps cyberspace is not quite as "traditional" as Congress's affirmation of authority might suggest; cyberspace is plainly different.

While this new cyberspace authority is viewed as an "affirmation" meant to clarify the existing covert action legal framework, it effectively created an entirely new one for cyberspace operations; it is an important difference in thinking about military cyberspace operations to suit the new threats faced by great power competition.[244] This "new" framework and thinking comes with changing the previously accepted practice of cyber operations: no longer delaying approval of operations due to disputes about whether they are covert operations;[245] altering the level of executive checks on secret operations; and opening the aperture on far more covert operations

[241] Chesney, *supra* note 17, at 599–600.
[242] JP 3-0, *supra* note 115, at xx; *see also* Nakashima, *supra* note 237.
[243] Nakashima, *supra* note 237. Practically speaking, much of the military activities involved in cyberspace to combat great power competition would likely have to be categorized as deterrence activities, amounting to overall strategic deterrence of the threat.
[244] *See id.*
[245] *Id.*

in the fifth domain that the military can conduct without the same extensive executive, congressional, and public oversight demanded years ago.

Congress has clearly anointed the military—specifically, U.S. Cyber Command and its subordinate units—as the agency of choice to lead the charge with secret operations, conducted on a near daily basis, to combat against great power competition. Despite Congress's rhetoric of calling these authorities an "affirmation," they permit sweeping changes in the manner of conducting operations, and they will shape how America, its allies, and its adversaries view conflict as a whole going forward. Cyberspace operations have clearly taken their place as the new norm of conflict, rather than an afterthought in planning.[246]

*5. A Modified Oversight Framework*

All of this is not to say that there is a complete lack of oversight over this sweeping range of permissible cyberspace activities. Although the extent of required executive branch checks has changed, there is still a degree of congressional oversight, though slightly less and different.[247]

Transparency of cyberspace operations first started in 2013, when Congress required quarterly briefings for all offensive and significant military operations in cyberspace.[248] In 2017, Congress imposed a new quarterly requirement for the Secretary of Defense to notify the Armed Services Committees on the application of the DoD's weapons review process for cyber tools and capabilities.[249] Additional congressional oversight provisions were included in the FY 2018 and FY 2019 NDAAs, which set up a modified oversight framework for cyberspace operations.

Pursuant to 10 U.S.C. § 395, a product of the FY 2018 and FY 2019 NDAAs, the Secretary of Defense must report "sensitive military cyber operations" (SMCOs) within forty-eight hours of the operation to the Senate

---

[246] Pomerleau, *supra* note 239.

[247] *See* Robert Chesney, *Covert Military Information Operations and the New NDAA: The Law of the Gray Zone Evolves*, LAWFARE (Dec. 10, 2019, 5:03 PM), https://www.lawfareblog.com/covert-military-information-operations-and-new-ndaa-law-gray-zone-evolves.

[248] *See* National Defense Authorization Act for Fiscal Year 2013, Pub. L. 112-239, sec. 939(a), § 484, 126 Stat. 1632, 1888 (codified at 10 U.S.C. § 484).

[249] *See* National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91, sec. 1631(a), § 130k, 131 Stat. 1283, 1737 (2017).

and House Armed Services Committees, mirroring the congressional notification requirements under the WPR.[250] Congress defined SMCOs under this provision as those military cyber operations that are meant to cause effects outside zones of hostilities or with respect to the involvement of the U.S. Armed Forces in hostilities not acknowledged publicly by the United States.[251] Congress likely added this immediate reporting requirement with the understanding that such cyber operations could have the potential to trigger larger scale conflict—perhaps with only the stroke of a keyboard. Thus, Congress required notification through the Armed Services Committees pursuant to its congressional war-making authority. The reporting requirement is remarkably the only outside check on the executive for activities conducted outside anticipated or ongoing hostilities. Congressional intent for reporting, however, is vague and not clearly defined in the Senate or House reports for the categories of SMCO,[252] leaving much of the determination regarding what qualifies as a SMCO to executive branch discretion. This reporting requirement becomes ripe for congressional modification in future NDAAs or to agencies for internal policy interpretation.

Of note, the FY 2020 NDAA narrowed the definition of SMCOs.[253] For operations to be reported, they must now meet a certain level of medium to high risk,[254] "eliminate[ing] relatively unimportant, low-risk operations from the scope of the notification obligation,"[255] even though they may still be undertaken outside areas of hostilities. This categorical elimination further limits the amount of cyberspace activities conducted by the military outside of anticipated or ongoing hostilities that are reported to Congress. Perhaps Congress became inundated with reporting on cyber operations after passing the FY 2019 NDAA "affirmation" of authority allowing for more secret military cyberspace operations and decided to reduce such reporting requirements. Whatever the motivation, this modification further

---

[250] 10 U.S.C. § 395; Robert Chesney, *Military Cyber Operations: The New NDAA Tailors the 48-Hour Notification Requirement*, LAWFARE (Dec. 18, 2019, 9:22 AM), https://www.lawfareblog.com/military-cyber-operations-new-ndaa-tailors-48-hour-notification-requirement.

[251] Chesney, *supra* note 250; *see also* H.R. REP. NO. 115-200, at 274 (2018).

[252] *See, e.g.*, H.R. REP. NO. 115-404, at 1016–17 (2018) (Conf. Rep.).

[253] *See* National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1632, 133 Stat. 1198, 1745–46 (2019).

[254] 10 U.S.C. § 395(c)(1)(C).

[255] Chesney, *supra* note 250.

opens the aperture for less oversight of sensitive military cyber operations, as well as those operations conducted outside of hostilities generally.

In short, there is a form of oversight by the Armed Services Committees for SMCOs, which are the type of cyber operations that would likely fall within the category of operations that "may generate unintended-but-painful consequences, just as in the covert action oversight paradigm."[256] However, the oversight is certainty not equal to that of the more robust covert action oversight paradigm. That oversight paradigm would have required *all* covert operations to be reported to Congress—not limited by risk factor or sensitivity, additional reporting to the Intelligence Committees (as well as to the Armed Services Committees for military covert activities), and a presidential finding determination.

### C. Next Steps in Building the Framework: Secret Military Cyber Information Operations

Considerations regarding public domestic and international scrutiny for cyberspace operations might become even more concerning when involving a foray into influence operations or covert information operations. The FY 2019 NDAA failed to provide any positive authority regarding these operations. Instead, the law merely stated that the military could conduct cyber operations as TMA that were "in support of information related capabilities."[257] Such a sweeping statement did not provide much direction or clarification for the conduct of these types of operations. Government agencies were back to square one with perceived ambiguity in the statutory scheme for covert or secret cyberspace military information operations.

Additional guidance regarding these information operations was, however, addressed in the FY 2019 NDAA conference report. According to the report, "information-related activities" could include, "when appropriate and approved, military deception and psychological operations."[258] The report went on to caution and "recognize that information operations are particularly contested and controversial."[259] Yet, in the same paragraph, the conferees agreed that the DoD needed to "conduct aggressive information

---

[256] *Id.*
[257] 10 U.S.C. § 394(f)(B)(iii).
[258] H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.).
[259] *Id.* at 1050.

operations to deter adversaries."[260] Congress added the caveat that the "affirmation" of cyber authorities was not an authorization for "clandestine [(or what is statutorily defined as covert)] activities against the American people or of activities that could result in any significant exposure of the American people and media to U.S. government-created information."[261]

The lack of clear congressional direction in the FY 2019 NDAA for information operations was problematic. After witnessing the scope and activities involved in Russia's election interference in the United States' 2016 presidential election, it became much more challenging to argue against the fact that traditional information warfare was increasingly becoming inseparable in practice with cyberspace operations.[262] With this acknowledgement came the recognition that one of the main pillars of great power competition, or this evolving "shadow war," involved adversaries engaging in unacknowledged "information warfare"[263] campaigns on information platforms.[264] Social media, especially, became a prominent

---

[260] *Id.*

[261] *Id.*

[262] Nakashima, *supra* note 237. Nothing illustrates the divisive effects of such an information operations campaign better than Russia's interference in the 2016 U.S. presidential election. To carry out its interference, Russian intelligence agencies used trolling, doxing, and online bots to spread disinformation about the elections throughout social media. *See generally* Indictment, United States v. Internet Rsch. Agency LLC, No. 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[263] As an initial matter, it is important to understand that the concept of information warfare has taken on many identities. *See* U.S. DEP'T OF ARMY, TECHS. PUB. 3-13.1, THE CONDUCT OF INFORMATION OPERATIONS para. 1-1 (4 Oct. 2018); JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS (27 Nov. 2012) (C1, 20 Nov. 2014); U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 1–2 (2018); *see also Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment: Hearing Before the Subcomm. on Emerging Threats & Capabilities of the H. Comm. on Armed Servs.*, 115th Cong. 4 (2017) (statement of Matthew Armstrong, Associate Fellow, King's Centre for Strategic Communications, King's College London). Despite differing views of information warfare among public and private sector actors, information warfare can be generally understood to mean operations taking place below the threshold of armed conflict that include both military and Government operations to protect and exploit the information environment. THEOHARY, *supra* note 226, at summary. While these tactics can be both defensive and offensive, the concept of information warfare in the colloquial sense focuses more on the offensive measures used by Government and non-state actors to influence military, economic, or political sentiment and public discourse to achieve strategic geopolitical objectives. *See id.*

[264] *See generally* SINGER & BROOKING, *supra* note 12; Nakashima, *supra* note 237; Michael Carpenter, *Countering Russia's Malign Influence Operations*, LAWFARE (May 29, 2019) https://www.justsecurity.org/64327/countering-russias-malign-influence-operations.

medium for spreading false or misleading information to sow unrest in the public or create distrust in the Government, effectively threatening national security.[265] Congress and the intelligence community publicly recognized that these foreign, online influence operations would continue to grow and pose a significant threat to the security and stability of the United States.[266] To combat this aspect of great power competition, clear direction and authorities became essential for information operations, just as they were for cyberspace operations.

*1. Affirming Secret Military Information Operations in Cyberspace*

In late 2019, Congress took on this task by further building on its evolving legal framework for cyberspace operations in great power competition. It again "affirmed" the authority of the military to conduct secret cyberspace operations but clarified the authority to also conduct secret (i.e., including covert) cyber information operations as TMA. Approved in December 2019, section 1631 of the FY 2020 NDAA, entitled "Matters Relating to Military Operations in the Information Environment," affirmed the authority of the Secretary of Defense "to conduct military operations, including clandestine operations, in the information environment to defend the United States . . . including in response to malicious influence activities carried out against the United States or a United States person by a foreign power."[267] These activities would also be considered and designated TMA,[268] defined in essentially the same manner as secret cyberspace operations under 10 U.S.C. § 394.[269]

---

[265] *See* Indictment, *Internet Rsch. Agency LLC*, No. 1:18-cr-00032-DLF; *see also* Jack Goldsmith, *The Failure of Internet Freedom*, KNIGHT FIRST AMEND. INST. (June 13, 2018), https://knightcolumbia.org/content/failure-internet-freedom (stating that the weaponization of social media "called into question the legitimacy of the election and of the democratic system more broadly"). According to a September 2019 Oxford University report, some seventy countries have had some type of disinformation campaign, either domestically or from foreign influence, showing that these threats are far from receding. SAMANTHA BRADSHAW & PHILIP N. HOWARD, THE GLOBAL DISINFORMATION ORDER: 2019 GLOBAL INVENTORY OF ORGANIZED SOCIAL MEDIA MANIPULATION 2 (2019). The report shows that governments are mainly spreading disinformation "(1) to suppress fundamental human rights; (2) to discredit political opposition; and (3) to drown out political dissent." *Id.*

[266] S. REP. NO. 116-48, at 327 (2019).

[267] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1631(b)(1), 133 Stat. 1198, 1741 (2019) (codified at 10 U.S.C. § 397 note).

[268] *Id.* § 1631(c).

[269] *Id.* § 1631(c), (i)(3).

Congress again defined "clandestine" in section 1631 as what is traditionally known as "covert": "marked by, held in, or conducted with secrecy, where the intent is that the operation or activity will not be apparent or acknowledged publicly."[270] Such "clandestine" military information operations, however, had to be carried out under one of four conditions, three of which resembled those categories related to secret military cyberspace operations, as discussed above.[271] Congress added one additional area of activities for information operations, thereby greatly expanding its already broad scope: secret information operations taking place "in support of military operations short of hostilities and in areas where hostilities are not occurring for the purpose of preparation of the environment, influence, force protection, and deterrence."[272] In other words, if the military were to conduct secret information operations in cyberspace, they would essentially be considered TMA. The broad scope of operations provided by Congress left little to no military information operation in cyberspace untouchable from a TMA designation.

*2. Expanding Challenges for the Future of Cyber Operations*

Since the FY 2020 NDAA provisions for information operations seem to mirror those provided for cyberspace operations in the FY 2019 NDAA, the broad scope of this authority shares some of the same concerns as those discussed above for secret cyberspace operations under the new legal framework. Adding, or "affirming," these authorities for information operations, however, raises far more concerning issues that remain unsettled.

First among these concerns is whether there are now any tangible limits to the scope of secret military cyberspace and information operations. Combining these two authorities offers the military quite a sweeping range of authorized operations in cyberspace that span the spectrum of conflict without the attendant extensive oversight and executive checks that once applied under the covert legal framework. For example, information operations that Congress once thought imposed serious risk and required extensive oversight and accountability (e.g., influencing foreign public opinion),[273] and would not be considered routine military operations under

[270] *Id.* (codified as amended at 10 U.S.C. § 394(f)(1)(A)).
[271] *Id.* § 1631(i)(3)(B).
[272] *Id.* § 1631(i)(3)(B)(iv).
[273] Chesney, *supra* note 17, at 597.

the prior legal framework, now fall under the rubric of cyber TMA pursuant to this "clarifying" authority.

Another concern is that the level of internal decision-making checks on the executive may no longer be significant enough to match the sensitivity of such operations or to ensure lower-level decision-makers are precluded "from engaging in an unacknowledged operation other than during times of overt hostilities."[274] The FY 2020 NDAA leaves open the question of how these information operations will be controlled or checked by higher levels of command or, more generally, those within the executive branch. Currently, approvals and delegations of authority for such operations will fall under the less restrictive internal policy direction implemented by the previous administration, and will thus be open to fluctuation with the current administration. The FY 2020 NDAA authority for information operations also implicitly acknowledges that geographic and functional commands carry out this function.[275] This aspect of information operations may seem unsurprising, since such operations have typically been carried out at lower levels as traditional forms of information operation tactics.[276]

However, these affirmations of authority for information operations in cyberspace that might be carried out at lower levels of command without extensive oversight and executive checks should still give Americans, policymakers, and practitioners pause. The traditional information warfare tactics are not the same as those from the Cold War information or psychological operations tactics, nor are they similar to those used in the Iraq War. Information warfare in today's operating environment is not simply about dropping leaflets or distributing manuals to opposing forces in a contained foreign territory. Instead, "[t]he internet, social media and smartphones have vastly extended the reach and precision of [information operations] tactics."[277]

The concept of protecting American institutions and conversations against the "bleed over" or "blow back" of secret information operations

---

[274] *Id.* at 600.
[275] *See* National Defense Authorization Act for Fiscal Year 2020 § 1631(d)(2)(A).
[276] *Cf.* Chesney, *supra* note 17, at 596–98. Such operations typically included: "strategic deception operations, certain peacetime psychological operations, some advance support contingency operations, and certain elements of some counterintelligence operations." H.R. REP. NO. 101-725, at 34 (1990).
[277] Nakashima, *supra* note 237.

intended for audiences abroad is now a nearly unsustainable goal.[278] It is a goal that is surely open to manipulation or reinterpretation if such operations are to continue in a public forum.[279] Today, the internet, and social media in particular, serves as the modern "public square."[280] In an era of the platform economy and surveillance capitalism, information and data now flow with unrivaled abundance across borders.[281] With this understanding of the information environment, one must acknowledge that the new public square is not solely American, but global. As such, it becomes less and less feasible for information operations in cyberspace to avoid prohibited "bleed over" or "blow back" into the realm of U.S. persons' exercise of First Amendment activities and public discourse.[282]

As discussed above, Congress recognized this aspect of information operations in the 2019 FY NDAA House conference report and provided some guidance to limit these operations. These limits still leave a vast amount of room for interpretation, though. How the executive or military defines "activities *against* the American people or of activities that could result in any *significant* exposure of the American people and media to U.S. government-created information"[283] will drive the extent to which

---

[278] *Cf.* U.S. ARMY WAR COLL., INFORMATION OPERATIONS PRIMER: FUNDAMENTALS OF INFORMATION OPERATIONS 12 (2011) (describing the difficulty in conducting information operations in the global information environment).

[279] To be clear, this leaves a small window of opportunity for information operations that narrowly target individuals through the use of closed applications intended to avoid "bleed over" into the general public forum. Yet the interconnected relationship of communications and information today belies the fact that it is still foreseeable for any information to enter the global public forum.

[280] Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017). Facebook alone connects over 2.2 billion people worldwide. SIVA VAIDHYANATHAN, ANTISOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 10 (2018). As of 2019, the Pew Research Center estimated that seven in ten Americans use social media to connect with one another, a statistic that has continued to exponentially grow over the past decade. *Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media.

[281] *See generally* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133 (2017) (suggesting the concept of the platform economy). *See* ZUBOFF, *supra* note 12 (suggesting the concept of surveillance capitalism). Professor Zuboff defines this concept primarily as a "new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales," or a "new global architecture of behavior modification" and "origin of new instrumentation power." *Id.*

[282] *See also* U.S. ARMY WAR COLL., *supra* note 278 (describing restrictions implicated by the Smith-Mundt Act (1948) on Government information influencing the American public).

[283] H.R. REP. NO. 115-874, at 1050 (2018) (Conf. Rep.) (emphasis added).

Government-created information appears within American discourse in the new global public square.

This prompts a number of questions about the permissible scope of military information operations in cyberspace. Two primary questions include: whether information is *against* the American people if originally planted in "red cyberspace," or adversarial information platforms, but then "bleeds over" into the American conversation;[284] and when information results in a *significant* exposure of the American people or public. Exposure cannot be measured by any known metric, especially if information is not even known to the public as U.S. Government-created information to measure in the first place. And what of the question of denying exposure? Congress failed to address those information operations in cyberspace that might be intended to take information away from the public, where it is not about exposing Americans to information but rather a denial of information. These questions yield follow-on questions. How many Americans can be exposed to such information or information-related operations before it is considered significant exposure? Is exposure to one American sufficient? Who might be the proper authority for these decisions and what might be the proper oversight mechanism? These questions, among others, are largely unsettled. How these questions are answered will surely have far-reaching impacts.

Still, impacts from secret military information operations in cyberspace and how they are regulated may never truly reach the light of day, leaving the American public to never know how these questions are answered or how the conversation is potentially being altered by the U.S. Government. Is reporting only to the Armed Services Committees truly enough oversight, and are the reporting requirements sufficiently meaningful when the stakes are so high? These questions seem foreboding and might paint too grim of a picture. This is not to suggest that Congress needs to backpedal its grants or "affirmations" of cyberspace authorities. Rather, highlighting these questions is meant to expose the types of issues that Congress, policymakers, and practitioners must now consider and attempt to answer.

As the law currently stands, such considerations and decisions may fall more readily on practitioners and lower-level commanders, perhaps with

[284] See JP 3-12, *supra* note 164, at xii, for a brief description of red, blue, and gray cyberspace, as those terms are understood by the U.S. military.

limited administrative restraints by the executive.[285] Under the current statutory framework, the executive branch would have to put up internal restraints for most of the information operations, meaning they could be just as easily removed. Congress provided the formula for allowing the Defense agency or executive to internally make these considerations and establish restraints from the inside. If conflict escalates, however, Americans may have to worry about how far those restraints might go as it relates to the weighing of national security interests and the protection of their civil liberties.[286] In this respect, Congress may want to consider other mechanisms and proposals to supplement the authorities for cyberspace and information operations.

## IV. Considerations and Proposals for the Fifth Fight in Great Power Competition

### A. Examining the Nature of Conflict and Balancing Instruments of National Power

#### *1. Norm-Building and Diplomacy*

One of the main concerns with the new legal framework for secret military cyberspace and information operations referenced throughout this article is whether any of these operations will ever be sufficiently in the domestic and international public view for scrutiny, attribution, or norm-building. Secret operations do not facilitate public acknowledgement and related norm observation,[287] aspects required for moving toward consensus

---

[285] To be clear, neither section 1631 of the FY 2020 NDAA nor 10 U.S.C. § 394 state in the definition of clandestine cyber and information operations that they are authorized by the President or Secretary of Defense. The level of this authorization for overall operations versus specific operations, however, is left to vast executive discretion and administrative changes without Congress specifying a scope of executive checks, as is the case with a covert action presidential finding. This is what leads to policy guidance that provides further delegations and loose restrictions that can be interpreted and changed between different administrations. *See* discussion *supra* Section III.B.4 (discussing the revocation of Presidential Policy Directive 20).

[286] One might compare this situation to how restraints for domestic surveillance were put up from the insides and easily taken down to effectuate a power grab by the executive branch, especially during times of crisis. *See* FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR 251 (2016).

[287] *See Cyber Policy Expert Speaks at the 2021 USCYBERCOM Legal Conference*, U.S. DEP'T OF DEF., https://dod.defense.gov/News/Special-Reports/Videos/?videoid=785814 (last visited Oct. 10, 2021).

on creating a more stable and secure cyber domain.[288] Norm-building and adherence play an important role in reducing risks to stability and security by increasing predictability and shaping responsible State behavior.[289] The United States' commitment to the international rules-based order through adherence to norms and continual norm-building through State practice ultimately contributes to the prevention of conflict.[290] Thus, the U.S. Government must be cautious not to overly rely on secret military operations—now a more readily accessible option in confronting great power competition. Military power must be balanced with other aspects of national power.

Diplomacy, for example, may still go the longest way in general conflict deterrence, especially with nations committed to complying with international law.[291] It is also a particularly critical aspect of national power in addressing malicious cyberspace activities. This is the case

---

[288] *Cf.* WHITE HOUSE, INTERIM NATIONAL SECURITY STRATEGIC GUIDANCE 9 (2021) (espousing that national security requires the United States to "lead and sustain a stable and open international system, underwritten by strong democratic alliances, partnerships, multilateral institutions, and rules"); WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 8 (2011) [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE] (declaring that the United States will work to "promote an *open, interoperable, secure, and reliable* information and communications infrastructure" and will do so by "build[ing] and sustain[ing] an environment in which *norms of responsible behavior* guide states' actions, sustain partnerships, and support the rule of law in cyberspace").

[289] *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 288, at 9.

[290] *See Joint Statement on Advancing Responsible State Behavior in Cyberspace*, U.S. DEP'T OF STATE (Sept. 23, 2019), https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace; *see also* ANGUS KING & MIKE GALLAGHER, CYBERSPACE SOLARIUM COMMISSION REPORT 3 (2020) (describing one of the pillars to implementing a national cyberspace strategy included strengthening norms and non-military tools).

[291] DAVID MAYERS, GEORGE KENNAN AND THE DILEMMAS OF US FOREIGN POLICY 106 (1990). Note, though, that there will be varying degrees of success for diplomacy to foster norm-building depending on whether nations are committed to complying with international law in the first place. In other words, there will be a large difference between Russia or China as near-peer competitors and rogue countries like North Korea and how they want to be perceived in the international sphere. However, neither differing degrees of compliance nor the effect norms have on nations should mean that the United States must discredit norm-building altogether. Instead, it should be perceived in such cases as just requiring a different calculus for each country. Further, much of norm-building and adherence is about strengthening alliances and international partnerships that can further facilitate combatting malicious cyberspace activities. That is to say that diplomacy to foster norm-building in cyberspace during great power competition should not be dismissed. *Cf.* James Andrew Lewis, *Five Cyber Strategies to Forget in 2021*, CTR. FOR STRATEGIC & INT'L STUD. (Dec. 3, 2020), https://www.csis.org/analysis/five-cyber-strategies-forget-2021.

because States are still trying to understand and reach a consensus on how international rules and norms apply, given emerging technology and a changing information environment that lacks historical precedent.[292] Engagement in this context, therefore, becomes essential to developing, sustaining, and maintaining those agreed-upon norms of responsible behavior to "guide states' actions, sustain partnerships, and support the rule of law in cyberspace."[293] Such engagement and development cannot be achieved through cloaks of secrecy.

Major aspects (or tools) of diplomacy include public attribution and international norm development, as well as related agreements or treaties between nations that help create incentives for, and build consensus around, a shared strategic vision for a peaceful international environment.[294] The United States recognizes attribution as essential for international norm-building and deterrence in the cyber context that requires a whole-of-government approach.[295] Premised on an understanding that nations want to be viewed as compliant with international law, public attribution for cyber attacks is thought to be an effective means to deter nations from committing attacks in the first place.[296] Public attribution and norm development are highly interdependent, though. Norms only develop into recognized legal requirements over time when States publicize them or use pubic attribution to criticize States that violate agreed-upon norms.[297] Norms

---

[292] *See, e.g.*, BRUNO LÉTÉ & PETER CHASE, SHAPING RESPONSIBLE STATE BEHAVIOR IN CYBERSPACE 8 (2018) (discussing how some States still voice concerns about the ambiguities in international law and debate about its actual scope as it relates to cyberspace).

[293] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 288; *cf.* JOINT CHIEFS OF STAFF, JOINT DOCTRINE NOTE 1-18, STRATEGY, at II-5 (25 Apr. 2018) (declaring the essence of the diplomatic instrument of national power as "engagement—how a nation interacts with state or non-state actors, generally to secure some form of agreement that allows the conflicting parties to coexist peacefully") [hereinafter JDN 1-18].

[294] *Cf.* JDN 1-18, *supra* note 293.

[295] *See, e.g.*, U.S. DEP'T OF JUST., *supra* note 263, at xiii ("Without attribution, there will be no consequences for offenders, and thus no deterrence."); WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 21 (2018) (recognizing the need for "swift and transparent consequences" to achieve deterrence in cyber operations).

[296] *Cf.* John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 422–23 (2016).

[297] *See* Melissa Hathaway, *When Violating the Agreement Becomes Customary Practice*, *in* GETTING BEYOND NORMS: NEW APPROACHES TO INTERNATIONAL CYBER SECURITY CHALLENGES 5–9 (Fen Osler Hampson & Michael Sulmeyer eds., 2017); *see* Carlin, *supra* note 296 (discussing how public attribution is essential where the United States seeks to persuade the international community of a norm of behavior).

are not just implemented, however; they must first be observed.[298] Hence, the United States' use of diplomacy, as well as the information element of national power, are critical tools to publicly inform and facilitate the evolving international discourse surrounding cyberspace activities.

Achieving success in diplomacy or informational power,[299] however, could become more of a challenge given the scope and potential effects of the new authorities for secret military cyber operations. This consideration needs to be at the forefront of authorizing all such secret military cyberspace operations. If the United States utilizes these military authorities to increase its robust engagement "in retaliatory covert or clandestine responses, those responses cannot contribute to deterrence against the many third parties

---

[298] Lewis, *supra* note 291. Though, one must consider that the process of how international norms seep into domestic law is convoluted and highly debated. Yet "scholars repeatedly conclude that domestic salience is crucial to many cases of states' compliance with international norms." Andrew P. Cortell & James W. Davis, Jr., *Understanding the Domestic Impact of International Norms: A Research Agenda*, 2 INT'L STUD. REV. 65, 67 (2000). Scholars and researchers in this area readily admit that it is extremely difficult to determine exactly why some norms are more salient than others in domestic structures. *See, e.g.*, *id.* Despite this difficulty, scholars have at least articulated that the first signs of international norms having a domestic impact is the appearance in domestic political discourse, changes in national institutions, and analysis of the State's policies. *Id.* at 69. In other words, these avenues may provide international norms a means for becoming more salient in a domestic legal structure or serve as evidence that they have already become salient within that structure. *See id.* Exactly how international norms are introduced and embedded into these features of the State's domestic politics is even more perplexing. *Id.* at 73. The important point to know, rather, is domestic or international impact cannot begin without States first acting to shape those norms through their own visible action and implementation of those norms and rules in their domestic legal systems. *Cf. 1 Year Anniversary of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, NETH. MIL. L. REV. https://puc.overheid.nl/mrt/doc/PUC_248137_11/1 (last visited Oct. 10, 2021) (arguing that cyber norm development can only be accomplished through States' adoption of treaties or by engaging in practices that when combined with expressions of state practice results in the crystallization of customary international law).

[299] The information instrument or element of national power is highly interrelated to diplomacy. According to joint military doctrine, a primary effect created to achieve a State's strategic informational objectives is communication synchronization, which entails

> focused efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of national interests, policies, and objectives. It actively engages key audiences with coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. Public diplomacy is good example of strategic communication.

JDN 1-18, *supra* note 293, at II-6.

who are watching, and indeed in context detracts from it."[300] Operations conducted in the dark have a tendency to stay there unless forced out by other mechanisms. The combination of reduced congressional oversight mechanisms and executive checks and the ability of the military to operate more freely in secret, in areas where there are no open hostilities, and with lower-level approvals combines to make the proposition for sufficient and meaningful public, congressional, and international scrutiny and norm-building less plausible. The instrument of military power, therefore, must now be more carefully considered and balanced appropriately with other instruments, and those considerations may reach down to the operational and perhaps tactical levels of military command. Further, the DoD must also internally balance the role it plays in secret operations and the role it plays in advancing diplomatic partnerships with foreign militaries.[301] The two roles may not always be mutually supporting.

The counterargument, of course, is that States are comfortable with a lack of norms and public attribution in cyberspace because it allows more latitude to maneuver.[302] Creating this "gray maneuver space" for military forces, however, also creates the maneuver space for America's adversaries. It has the potential to hamper the development of other instruments of national power. If the strategic end state for America is to create stability and security in cyberspace, the line for increasing secret military cyberspace activities must be drawn somewhere. Otherwise, the Nation runs the risk of facilitating the destabilization and militarization of cyberspace—feeding into a strategic narrative that runs completely counter to American values of an open, secure, and free internet that is supported by democratic ideals.[303] And this is what America's adversaries—especially China—want.[304]

---

[300] JACK GOLDSMITH & STUART RUSSELL, HOOVER INST., AEGIS SERIES PAPER NO. 1806, STRENGTHS BECOME VULNERABILITIES: HOW A DIGITAL WORLD DISADVANTAGES THE UNITED STATES IN ITS INTERNATIONAL RELATIONS 13 (2018).

[301] *Cf., e.g.*, PANAYOTIS A. YANNAKOGEORGOS, STRATEGIES FOR RESOLVING THE CYBER ATTRIBUTION CHALLENGE 6 (2016); *see generally* DOD CYBER STRATEGY SUMMARY, *supra* note 8 (noting the DoD's mission includes working with foreign allies and partners to contest cyber activity).

[302] *See, e.g.*, LÉTÉ & CHASE, *supra* note 292.

[303] *See* Goldsmith, *supra* note 265; *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, *supra* note 290.

[304] *Cf., e.g.*, Bret Austin White, *Reordering the Law for a China World Order: China's Legal Warfare Strategy in Outer Space and Cyberspace*, 11 J. NAT'L SEC. L. & POL'Y 435 (2021). *See generally* Jinghan Zeng et al., *China's Solution to Global Cyber Governance: Unpacking*

Great power competitors want to both erode and reshape the post-1945 international order.[305] America may be permitting this by remaining silent and increasing its secret military operations in cyberspace at the expense of other instruments of national power, thus feeding into competitors' ability to reshape the American strategic narrative.[306] Ultimately, this adversarial counter-narrative erodes the American public's trust in democratic government and institutions; it is the end goal of America's most capable and powerful adversaries in great power competition.[307] The narrative that America is simply "policing" malicious activities in cyberspace at an ever-increasing scale can only go so far without sufficient transparency or accountability to the American public and international States and actors before it is put into question and works against America's strategic objectives. Advancing America's strategic narrative requires a delicate balancing act. While the military may be able to spearhead many cyberspace and information-related activities, and now has far more latitude to do so with new authorities, U.S. Government decision-makers must proceed cautiously and ensure such use of the military is appropriately reserved and balanced with other instruments of national power that may be far more critical in terms of long-term strategic competition.[308]

*2. The Prospect of Escalation*

The prospect of escalation becomes equally concerning given the new legal framework for secret military cyber operations. The new authorities demonstrate that Congress is no longer heeding the Church Committee's

---

*the Domestic Discourse of "Internet Sovereignty"*, 45 POL. & POL'Y 432 (2017) (discussing China's use of sovereignty and norms in cyberspace to compete with the U.S. position on an open and free internet); Roza Nurgozhayeva, *Rule-Making, Rule-Taking or Rule-Rejecting Under the Belt and Road Initiative: A Central Asian Perspective*, 8 CHINESE J. COMP. L. 250 (2020).

[305] *See, e.g.*, Lewis, *supra* note 291.

[306] *Cf.* Goldsmith, *supra* note 265.

[307] *See id.*; discussion *infra* Part I (discussing great power competition and adversarial end goals).

[308] *See Cyber Policy Expert Speaks at the 2021 USCYBERCOM Legal Conference*, *supra* note 287; Interview by John J. Hamre & Seth G. Jones with Robert M. Gates, Former Sec'y of Def., in Washington, D.C. (June 17, 2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200618_Exercise%20of%20Power.pdf. Former Secretary of Defense Gates argued in 2020 that this new strategic competition needs to focus on other areas of national power rather than exclusively on the military aspect of power—that focusing too much on the military aspect may have actually set the United States up for disarray in our international relations. *See id.*

warning that vigorous checks are required for such secret high-risk activities to prevent war.[309] Scholars, however, have warned that increasing authorities, flexibility, and freedom of movement for military cyberspace operations will likely result in conflict escalation and could place too much emphasis on military tools to combat great power competition in cyberspace, conceivably missing the true character of this new conflict.[310] Involved here is the concern that military and Government leaders might fixate on technology and move to a more offensive posture at the expense of more helpful but difficult policy choices.[311] A recent military study shows that while the historical acquisition and use of cyber technology alone may not be enough to drive escalation, accompanying policy decisions can.[312] Thus, coupling evolving cyber tools and increasingly escalatory policy to accompany increased operational authorities may drive toward escalation and destabilization.

To be clear, the concern regarding escalation toward major armed conflict is waning.[313] Experts have concluded that States are continuing to exhibit a respect for the threshold of armed conflict in great power competition and structure their activities accordingly; States actively avoid direct conflict in advancing their objectives.[314] Rather, the concern is of escalation in the sense of continued increasing military operations to create effects or impose costs in a persistent and continuous cycle that

---

[309] 1 S. REP. NO. 94-755, at 613 (1976).
[310] Brandon Valeriano & Benjamin Jensen, *The Myth of the Cyber Offense: The Case for Restraint*, CATO INST. (Jan. 15, 2019), https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint; MORRIS ET AL., *supra* note 6, at 153; *see also* Interview with Robert M. Gates, *supra* note 308 (arguing that other elements of national power need to be at the forefront of confronting strategic competition).
[311] *Cf.* Shira Ovide, *Technology Will Not Save Us*, N.Y. TIMES (Apr. 29, 2020), https://www.nytimes.com/2020/04/29/technology/coronavirus-contact-tracing-technology.html; Jacquelyn Schneider, *The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War*, 42 J. STRATEGIC STUD. 841, 842 (2019) ("[I]ncreases in highly centralized networks and the proliferation of digital vulnerabilities within civilian infrastructure, combined with a continued belief in offense dominance, could increase incentives for first strike over time.").
[312] *See* Caitlin Talmadge, *Emerging Technology and Intra-War Escalation Risks: Evidence from the Cold War, Implications for Today*, 42 J. STRATEGIC STUD. 864, 869–70, 875 (2019).
[313] Lewis, *supra* note 291.
[314] *E.g.*, *id.*

tends to militarize cyberspace[315] at the expense of other instruments of national power, public messaging, and public-private domestic defense cooperation.[316] Increasing these activities at scale and duration with the military at the helm tends to lead to such a narrative. Such increasing activities can also lead to increased shutdowns in accesses to networks or forms of surveillance that tangentially effect civilian populations (short of crossing the threshold of armed conflict), which begets destabilization and decreases cooperation with domestic private entities. Stability becomes less attainable, and the prospect for unintended consequences that could be devastating and trip the threshold of armed conflict increases.[317] The United States should be concerned about this form of escalation.

Accordingly, the impact of increasing authorities, flexibility, and freedom of maneuver for the military by changes in both policies and law, in the context of great power competition, heightens concerns for escalation. The increasing possibility of escalation is even more precarious in this context since operating in this domain has the greatest potential to affect U.S. persons' civil liberties (such as freedom of speech, the related right to receive speech, and the constitutional right to privacy), potentially beyond public view.[318] If not properly checked and balanced by public acknowledgement and other instruments of national power, secret military cyberspace activities can be a major driving force in the direction toward destabilization rather than norm-building and cooperation. The U.S. Government already learned this lesson during the initial stages of the Cold War, when Congress and the public stepped in and demanded changes in the legal framework to address authorities, flexibility, and freedom of maneuver for secret activities by Government agencies.[319] The fact that Congress shifted so extensively from its Church Committee-era position on covert operations outside of open hostilities in cyberspace creates a

---

[315] *See* Nakasone & Sulmeyer, *supra* note 213 (recognizing that the persistent engagement doctrine and "defend forward" strategy that involves imposing costs in cyberspace can lead to escalation and must be taken seriously as a concern and planned for accordingly).
[316] *See generally Cyber Policy Expert Speaks at the 2021 USCYBERCOM Legal Conference*, *supra* note 287.
[317] *Cf. id.*
[318] *Cf.* DONOHUE, *supra* note 38, at 24–26 (discussing how citizens gave up significant privacy rights in the name of national security after responding to 9/11 and the war on terrorism, such as through the enactment of the USA PATRIOT Act that increased the scope of permissible Government surveillance); *see generally* Joseph Thai, *The Right to Receive Foreign Speech*, 71 OKLA. L. REV. 269 (2018).
[319] *See* discussion *supra* Section II.A.2.

fascinating paradox. Yet, this is exactly the new legal and operational landscape that America has entered into with the fifth fight.

B. Examining Accountability and Responsibility

*1. Oversight Mechanisms*

Oversight mechanisms can help to balance the military instrument of power in confronting great power competition and to increase public acknowledgment through congressional representation. Ensuring meaningful and robust congressional oversight is also most critical when highly classified covert action or clandestine policy and programs often have little visibility outside of Congress; therefore, this oversight and form of "public acknowledgement" is one of the few meaningful checks on the executive in this area.[320] This is not to suggest, however, that the current mechanisms are failing; it is almost too soon to know their effectiveness in properly checking the executive branch and informing Congress and the public. Nevertheless, based on historical precedent and concerns for tempering secret Government activities generally, some analogies and suggestions can still be made to improve the current structure.

Rather than looking back to Cold War-era guidance on oversight and addressing public outcry over secret Government activities, an interesting analogy can be made with more recent events. Public outcry over the secret activities of the NSA's bulk data and metadata collection program, exposed after the Edward Snowden leaks[321] serves as a palpable guidepost for suggestions to an oversight framework for secret cyberspace activities. The bulk data collection program was facilitated by changes in the legal framework under section 702 of the FISA Amendments Act and section 215 of the USA PATRIOT Act.[322] Working in tandem, these provisions created avenues for undermining U.S. citizens' rights, along with sobering implications for America's democratic narrative supporting an open and free internet.[323] Similar to the changes in the legal framework for secret military cyberspace operations, these bulk data collection provisions were implemented to address emerging global threats to the United States and

[320] DEVINE, *supra* note 45, at 1.
[321] *See* DONOHUE, *supra* note 38, at 38.
[322] *See id.* at 4–9.
[323] *See generally id.*

confront new technology in cyberspace along with a changing information environment.[324]

In 2016, Professor Laura Donohue suggested changes to the oversight mechanism for foreign intelligence collection following the exposure of the U.S. Government's use of the bulk data collection program.[325] She argues that adding more oversight to the process of checking the implementation of section 702 and section 215 would not resolve the underlying constitutional concerns,[326] nor would increasing executive branch reporting to Congress likely achieve the appropriate amount of public acknowledgment since a myriad of reporting requirements already existed.[327] Instead, Professor Donohue argued, more *robust* oversight was required,[328] including the restoration of term limits on committee members to ensure "Congress casts a more critical eye on executive branch activities—and that more members of Congress participate, making oversight more representative."[329]

Expanding on Professor Donohue's suggestion, Congress might also consider changes to the committee and its scope. In particular, Congress needs to examine whether the reporting and oversight for secret military cyberspace activities rests with the appropriate committees and whether the appropriate committees even exist.[330] Reporting to the Senate and House Armed Services Committees certainly makes sense, in that most of these cyberspace operations are in support of larger military efforts and must be considered holistically. Further, the Armed Services Committees have subcommittees that consider and focus on cyberspace matters.[331] But

---

[324] *See id.* at 24–25, 33–34.
[325] *See id.* at 136–50.
[326] *Id.* at 138.
[327] *See id.* at 137.
[328] *Id.* at 138. In other words, the problem is not necessarily always needing to report to more committees, thereby creating a redundancy problem of social shirking where groups then may be less prone to take responsibility. *See id.* at 136–37.
[329] *Id.* at 139.
[330] One of the main recommendations from the Cyberspace Solarium Commission Report was reforming the U.S. Government's structure and organization for cyberspace, to include improving its oversight of cybersecurity by reorganizing and centralizing its committee structure and jurisdiction. KING & GALLAGHER, *supra* note 290, at 31.
[331] *See U.S. Senate: Committee on Armed Services*, U.S. SENATE, https://www.senate.gov/general/committee_membership/committee_memberships_SSAS.htm#SSAS21 (last visited Sept. 30, 2021); *Cyber, Innovative Technologies, and Information Systems*, HOUSE

responsibility for those cyberspace matters is still dispersed throughout these numerous subcommittees, muddling oversight.[332] Limiting oversight to the military committees also likely results in members' deference to the military, potentially resulting in "benign neglect" and perhaps leading to missed opportunities to balance other instruments of national power.[333] Coupling concerns over deference and executive branch policies that no longer give other agencies accessible veto authority over military cyberspace operations potentially continues to work against balancing military power. The combination of these factors also leads to a perception, if not reality, that the oversight to the Armed Services Committees stovepipes reporting to the detriment of public accountability and a fully weighed whole-of-Government response to adversarial actions in cyberspace.

A new permanent congressional committee on cyberspace is one way to ensure all equities are considered and balanced appropriately for public acknowledgment. The U.S. Cyberspace Solarium Commission made a similar recommendation in 2020,[334] recommending the creating a House Permanent Select and Senate Select Committee on Cybersecurity that would mainly oversee cybersecurity policy and defensive operations.[335] However, the scope of jurisdiction and authorities for the proposed cybersecurity committees may still be too narrow. The commission did not intend to include activities already overseen by the Armed Services Committees.[336]

In contrast, a more broadly scoped House Permanent Select and Senate Select Committee on Cyberspace Matters that includes activities now overseen by the Armed Services Committees can focus on the unique characteristics of cyberspace more generally. The jurisdiction would include both defensive or cybersecurity matters and offensive cyber operations, which would account for the highly interrelated nature of these activities. It would also allow for a better balancing of all instruments of national power when considering holistic conduct in cyberspace from various Government agencies—improving a whole-of-nation approach. Broader scoped

---

ARMED SERVS. COMM., https://armedservices.house.gov/cyber-innovative-technologies-and-information-systems (last visited Sept. 30, 2021).

[332] KING & GALLAGHER, *supra* note 290, at 31.

[333] *Cf.* DEVINE, *supra* note 41, at 3; Van Wagenen, *supra* note 76, at 98–99.

[334] *See* KING & GALLAGHER, *supra* note 290, at 35–36.

[335] *Id.*

[336] *Id.* at 36.

cyberspace committees can better account for how cyberspace and information operations in this domain are interrelated and differ from those information operations of the past. Information operations carried out in cyberspace can have especially meaningful implications for citizens' rights. Accordingly, such information-related operations should be adequately accountable to the public within this structure as well rather than stove-piped within the Armed Services Committees.

Once Congress can see the bigger picture as it relates to defensive, offensive, and information operations, it can consider whether it is asking the right questions of the executive branch for robust and meaningful oversight. Answers to the right questions for reporting can provide more impactful input for public acknowledgement and better insights for the Government to consider the appropriate strategic balance to counter great power competition.

*2. Building Domestic and International Partnerships*

Congress's "affirmations" of authorities were intended to close one gap in the legal framework that informed America of its adversaries' malicious cyberspace activities. Military cyberspace and information-related operations can now counter adversaries with a range of flexible responses and keep pace with ever-evolving tactics, techniques, and procedures. On the other hand, the prospect for escalating secret military cyberspace and information-related operations increases, along with the prospect for losing important public acknowledgment of operations for norm-building and accountability. While internal executive branch policies and new oversight mechanisms may be the obvious means to address these issues, it is equally important to investigate other areas of the law that can work toward striking the right balance between operational needs and public acknowledgment. That is, where one seam in the legal framework is now closed, another may be more exposed.

One such gap may exist in the domestic legal framework that supports public-private cybersecurity information sharing and cooperation on domestic infrastructure. Increasing secret military cyberspace and information operations could hamper public trust and hurt efforts to build public-private cooperation at the home front.[337] Similarly, the military's

[337] *See* discussion *supra* Section III.B.3.

increase in secret, persistent, and more aggressive operations, combined with a lack of open information sharing about those operations and threats, could break down trust with international partners and hurt efforts to work together to counter threats and build international norms.[338] In order to balance these concerns and create more accountability to both foreign and domestic partners, as well as share in the responsibility for countering malicious cyber activities, laws and policies need to address increased information sharing and cooperation with these partners and the military.

To foster international partnerships, "hunt forward" operations, as part of the persistent engagement doctrine and "defend forward" strategy,[339] are a step in the right direction. The United States conducts these military cyberspace operations hand-in-hand with an international partner.[340] Doing so can build much needed trust and create space for norm development through combined activities. These operations, however, could benefit from U.S. laws that expand the permissible scope of information sharing, making for a more robust and meaningful partnership that builds trust and creates a shared responsibility for countering cyberspace threats. Increased information sharing and more robust partnerships also signal to adversaries America's resolve to work with the international community, remain accountable, and build norms together.

To that end, Congress should consider improving the military's ability to share cyberspace capabilities, information, and related data with international partners. Intelligence agencies, such as the NSA and the National Geospatial-Intelligence Agency, have special authorities that allow for more permissive capability or information sharing and support with foreign partners.[341] But no such authority exists—outside perhaps the long, arduous, and unclear process of arms control and foreign military sales—for the military (i.e., U.S. Cyber Command and subordinate units), the entity now primarily conducting operations with foreign partners in cyberspace. If one legal framework has changed to account for the speed and changing

---

[338] *See, e.g.*, Max Smeets, *Cyber Command's Strategy Risks Friction with Allies*, LAWFARE (May 28, 2019, 7:50 AM), https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies ("U.S. Cyber Command's mission to cause friction in adversaries' freedom of maneuver in cyberspace may end up causing significant friction in allies' trust and confidence—and adversaries may be able to exploit that.").

[339] *See, e.g.*, *DOD Has Enduring Role in Election Defense*, *supra* note 214.

[340] *See, e.g.*, *id.*

[341] *See* 10 U.S.C. §§ 421, 443.

nature of cyberspace, then others should follow suit. Otherwise, the United States stands to lose the benefits of those newly granted military authorities.

Congress should likewise focus its efforts on improving information sharing between the military and private sector to strengthen domestic partnerships. Establishing partnerships with private sector and the military is especially important when information is related to foreign adversarial activities in cyberspace. Insights into foreign threat actors and activities operating on domestic infrastructure can facilitate the military's efforts to counter those threats abroad, before they even reach the United States.

Over the years, Congress has gradually assisted in establishing a legal framework that can facilitate domestic public-private information sharing. Major legislative efforts, like the Cybersecurity Information Sharing Act (CISA) of 2015, provide private entities liability protection and mechanisms for information sharing with the Government about "cyber threat indicators" and "defensive measures."[342] However, the private entity information-sharing mechanisms established through CISA's authority is very limited and has its continued challenges.[343]

One key challenge for private-public information sharing through CISA is that private entities must report threat information through the Department of Homeland Security's threat reporting system or else risk losing the protections CISA affords.[344] Reporting to other Government agencies, such

---

[342] S. 754, 114th Cong. § 106 (2016); *see* S. REP. NO. 114-32, at 2–3 (2015).

[343] *See* OFF. OF THE INSPECTOR GEN. OF THE INTEL. CMTY., AUD-2019-005-U, UNCLASSIFIED JOINT REPORT ON THE IMPLEMENTATION OF THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, at 9–11 (2019) (addressing continued challenges of implementing the Cybersecurity Information Sharing Act of 2015 (CISA) for information sharing). Pursuant to CISA, threat indicators and defensive measures only include those cyber threats to networks and systems for cybersecurity protection. *See* S. 754 § 102(6), (7). While these threats are important to address for security purposes and data-related harms, it does fail to include content-related information operation threats that might be solely violating an information platform's terms of service, for instance. *See* S. REP. NO. 114-32, at 3–4; S. 754 § 102(5)(B). The failure to include information-related threats risks losing important indicators regarding ongoing information warfare campaigns.

[344] S. 754 § 105(c)(1)(B)(i)–(ii). Under CISA, "the only way to receive the liability protection of section 106 is to share information through the 'DHS capability and process' created under section 105(c), or through the exceptions covering follow-up communications and 'communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat.'" Brad S. Karp et al., *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. F. ON CORP.

as the DoD, would effectively strip private entities of CISA's protections, creating hesitancy for reporting. Private entities may not want to report through the Department of Homeland Security system, as it is distributed to all agencies, including law enforcement.[345] Such reporting may trigger consequences for the private entity's public perception, financials, and responsibilities to shareholders. Private entities may instead prefer to report directly to the military to assist in securing cyberspace without domestic law enforcement involvement. In such cases, Congress should not foreclose reporting mechanisms to Government agencies, as all reporting and information sharing is valuable. Increasing viable avenues for reporting can only work toward strengthening relationships and sharing in the responsibility to secure America's domestic infrastructure, making the nation more resilient to malicious activities.

## V. Conclusion

The history of covert action development is an important one. It demonstrated that Congress and the public are traditionally uneasy with secret activities conducted below the threshold of armed conflict. Such activities were typically thought to evade checks on the Government. After decades of legal and congressional reform following the Church and Pike Committee investigations, Congress placed multiple checks on the conduct of covert operations in peacetime. Those internal checks were effectuated through the WPR and the traditional covert action legal framework with its

---

GOVERNANCE (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015.

[345] The Cybersecurity Information Sharing Act of 2015 required the appropriate Federal entities to develop guidelines for information sharing with private entities. S. 754 § 103(a). The Federal entities, led by the Department of Homeland Security, published Federal guidelines that established the Automated Information Sharing (AIS) system as the primary mechanism to share unclassified threat information with private entities and Federal entities. *See* OFF. OF THE DIR. OF NAT'L INTEL. ET AL., SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2016). While the Department of Defense is not precluded from utilizing other sharing mechanisms outside of the AIS system to share information with private entities, the private entities themselves have less flexibility for information sharing with the Federal Government if they want to avail themselves of CISA's protections. *See* S. 754 § 105(c)(1)(B)(i)–(ii). Further, when information is shared through AIS, one of the guiding principles of CISA, as implied through the law, is that the information will be distributed amongst Federal entities as widely as possible, which may not be appealing to some private entities worried about law enforcement involvement. *See* OFF. OF THE DIR. OF NAT'L INTEL. ET AL., *supra* note 345; *see also* S. 754 § 105(a)(3)(A)(i)–(iii).

attendant extensive oversight, decision-making, and reporting requirements. Similarly, external checks on the Government were implemented through enlightening public opinion by requiring the conduct of overt operations in situations considered traditional military activities that would fall outside the covert action legal framework. Conflict was subsequently restrained, and there was extensive accountability and responsibility mechanisms baked into the legal framework.

Despite this history, this is no longer the case for activities in cyberspace. Secret cyberspace operations, both offensive and defensive, and cyber information operations now make up activities referred to in this article as the fifth fight, which now has its own legal framework. With the title of "affirmations" of authority, the practical reality is that this new legal framework for secret cyber and information operations brings with it sweeping changes and significant implications that will shape the future nature of conflict, accountability, and responsibility. Policymakers must consider this critical stage of conflict we have entered and the Nation's shifting national security priorities. The legal landscape has opened a clear path for fast-paced, secret, constant, and persistent engagements in cyberspace—hopefully giving the United States the edge it needs to combat this new shadow war. The fifth fight may, however, ultimately be a destabilizing fight without the careful balance of tempering executive policies and decision-making processes, weighing where authorities should rest, meaningful congressional oversight, and efforts to create public and partner trust and transparency.

If nothing else, this article is meant to bring these considerations into the forefront of discussion when considering the future of great power competition and highlight how the locus of that fight has shifted into cyberspace, creating the fifth fight and its unique legal challenges.