Volume 229 Issue 3 2021

MILITARY LAW REVIEW

Articles

The Rise of the "Fifth Fight" in Cyberspace: A New Legal Framework and Implications for Great Power Competition
Major Laura B. West

Targeting Submarine Cables: New Approaches to the Law of Armed Conflict in Modern Warfare
Lieutenant Commander Dennis E. Harbin III

Medals "Ridiculously Given"? The Authority to Award, Revoke, and Reinstate Military Decorations in Three Case Studies Involving Executive Clemency
Dwight S. Mears

Lecture

The Thirty-Seventh Charles L. Decker Lecture in Administrative and Civil Law: Military Law in Uncertain Times
Edwin Meese III

Academic Journal No. 27-100-229-3

Military Law Review

Volume 229 **Issue 3** **2021**

CONTENTS

Articles

The Rise of the "Fifth Fight" in Cyberspace: A New Legal Framework and Implications for Great Power Competition
Major Laura B. West *273*

Targeting Submarine Cables: New Approaches to the Law of Armed Conflict in Modern Warfare
Lieutenant Commander Dennis E. Harbin III *349*

Medals "Ridiculously Given"? The Authority to Award, Revoke, and Reinstate Military Decorations in Three Case Studies Involving Executive Clemency
Dwight S. Mears *381*

Lecture

The Thirty-Seventh Charles L. Decker Lecture in Administrative and Civil Law: Military Law in Uncertain Times
Edwin Meese III *431*

Headquarters, Department of the Army, Washington, D.C.

Academic Journal No. 27-100-229-3, 2021

Military Law Review
Volume 229
Issue 3

Since its inception in 1958 at The Judge Advocate General's School, U.S. Army, in Charlottesville, Virginia, the *Military Law Review* has encouraged a full and frank discussion of legislative, administrative, and judicial principles through a scholarly examination of the law and emerging legal precepts. In support of that mission, the *Military Law Review* publishes scholarly articles that are relevant to, and materially advance, the practice of law within the military.

The *Military Law Review* does not promulgate official policy. An article's content is the sole responsibility of that article's author, and the opinions and conclusions that are reflected in an article are those of the author and do not necessarily reflect the views of the U.S. Government,

the Department of Defense, the Department of the Army, The Judge Advocate General's Corps, The Judge Advocate General's Legal Center and School, or any other governmental or non-governmental agency.

WEBSITE: The *Military Law Review* is available online at https://tjaglcs.army.mil/mlr.

CITATION: Cite this issue of the *Military Law Review* as 229 MIL. L. REV. [page number] (2021).

MANUSCRIPT SUBMISSIONS: The *Military Law Review* accepts manuscript submissions from military and civilian authors. Any work submitted for publication will be evaluated by the *Military Law Review*'s Board of Editors. In determining whether to publish a work, the Board considers the work in light of the *Military Law Review*'s mission and evaluates the work's argument, research, and style.

No minimum or maximum length requirements exist. Footnotes should be numbered consecutively from the beginning to the end of the manuscript rather than by section. Citations must conform to *The Bluebook: A Uniform System of Citation* (21st ed. 2020) and the *Military Citation Guide* (24th ed. 2021). Submissions should include biographical data for each author, to include branch of service, duty title, present and prior positions or duty assignments, all degrees (with names of granting schools and years received), and previous publications. If submitting a lecture or paper prepared in partial fulfillment of degree requirements, the author should include the date and place of delivery of the lecture or the date and source of the degree.

Submissions must be in Microsoft Word format and should be sent via email to the Editor, *Military Law Review*, at usarmy.pentagon.hqda-tjaglcs.list.tjaglcs-mlr-editor1@mail.mil. If email is not available, please forward the double-spaced submission to the Editor, *Military Law Review*, Administrative and Civil Law Department, The Judge Advocate General's Legal Center and School, U.S. Army, 600 Massie Road, Charlottesville, Virginia 22903-1781.

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.

TARGETING SUBMARINE CABLES: NEW APPROACHES TO THE LAW OF ARMED CONFLICT IN MODERN WARFARE

LIEUTENANT COMMANDER DENNIS E. HARBIN III*

It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy. . . . [W]e have allowed this vital infrastructure of undersea cables to grow increasingly vulnerable. This should worry us all.[1]

I. Introduction

On 1 July 2019, fourteen Russian sailors tragically died when their submarine caught fire.[2] The submarine is the *Losharik*, an unarmed, nuclear-powered vessel designed to operate at depths greater than 10,000 feet.[3] According to U.S. officials,[4] the *Losharik* is not just an undersea research vessel, but also a submarine designed specifically to disrupt the "global infrastructure system that transmits 99 percent of the international data sent over the internet."[5] Its mission is to target submarine cables as a means to wage cyber warfare—at sea.

---

* Judge Advocate, United States Navy. Presently assigned to the Joint Staff. J.D., 2014, The Pennsylvania State University, Dickinson School of Law, Carlisle, Pennsylvania; B.A., 2008, Virginia Military Institute, Lexington, Virginia. A previous version of this article was submitted in partial fulfillment of the Master of Laws requirements of The Judge Advocate General's School, U.S. Army. This article was awarded the 2021 Richard R. Baxter Military Prize in recognition that it significantly enhances the understanding and implementation of the law of war. The author thanks the Lieber Society on the Law of Armed Conflict and the American Society of International Law for consideration and selection. The views expressed herein are solely those of the author and do not reflect the views or opinions of the Department of the Navy, the Department of Defense, or any other institution.

[1] James Stavridis, *Foreword* to RISHI SUNAK, UNDERSEA CABLES: INDISPENSABLE, INSECURE 9 (2017).

[2] Alexandra Ma & Ryan Pickrell, *The Russian Submarine that Caught Fire and Killed 14 May Have Been Designed to Cut Undersea Cables*, BUS. INSIDER (July 3, 2019, 8:33 AM), https://www.businessinsider.com/russia-submarine-losharik-undersea-cables-media-speculation-2019-7.

[3] *Id.*

[4] *Id.*

[5] Garrett Hinck, *Evaluating the Russian Threat to Undersea Cables*, LAWFARE (Mar. 5, 2018, 7:00 AM), https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.

In recent decades, academics and practitioners have spilled much ink discussing the character of warfare in the cyber age. Due to the unique aspects of the cyber battlespace, it continues to challenge national security law practitioners in the application of traditional law of armed conflict (LOAC) [6] principles, such as distinction and proportionality. The scholarship has focused primarily on the applicability of LOAC to either (a) operations that use cyber weapons to achieve cyber effects[7] or (b) operations that use cyber weapons to achieve tangible, kinetic effects. Missing from the discussion is how LOAC applies to a third form of cyber warfare:[8] military operations that use conventional weapons to achieve cyber effects.

One example of such a military operation is the 2019 Israeli Defense Force's bombing of a building containing Hamas hackers.

> The assault seems to be the first true example of a physical attack being used as a real-time response to digital aggression . . . . That makes it a landmark moment, but one that analysts caution must be viewed in the context of the conflict between Israel and Palestine, rather than as a standalone global harbinger.[9]

---

[6] This article uses the phrase "law of armed conflict (LOAC)" to refer to (a) the coherent system of the law of war principles (i.e., military necessity, humanity, honor, distinction, and proportionality) and (b) treaties and customary State practice that relate to the means and methods of warfare, as well as the protection of civilians and their objects. *See* OFF. OF GEN. COUNS., U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL §§ 1.3, 2.1 (12 June 2015) (C3, 13 Dec. 2016) [hereinafter LAW OF WAR MANUAL].

[7] An effect is the "result, outcome, or consequence of an action." *See* JOINT CHIEFS OF STAFF, DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 69 (Jan. 2021).

[8] For the purposes of this article, "cyber warfare" is the conduct of military operations between belligerents that occur in the "cyber domain" or "cyberspace." Cyberspace is 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." *Id.* at 55.

[9] Lily Hay Newman, *What Israel's Strike on Hamas Hackers Means for Cyberwar*, WIRED (May 6, 2019, 4:43 AM), https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar.

Although the Israeli Defense Force strike may have been a "landmark moment," the United States reserved the right to retaliate against cyber attacks using conventional weapons as early as 2011.[10]

Regardless of whether the Israeli Defense Force's strike is isolated to only that conflict, this third form of cyber warfare could exist in other places and in other domains. Arguably, more threatening is the use of kinetic weapons, such as a deep-submersible submarine, to target submarine cables either in the opening salvos of a war or during the conflict. The only legally binding treaty in force today that relates to the targeting of submarine cables in wartime is the 1907 Hague Regulations, which pertain only to the seizure or destruction of submarine cables connecting occupied and neutral territories.[11] That treaty permits targeting submarine cables "in the case of absolute necessity."[12] Moreover, through historical precedent and the application of LOAC developed in the Industrial Age, submarine cables remain lawful targets.

In the cyber age, however, reliance by States and the civilian populations on submarine cables cannot be overstated. Approximately 400 garden-hose-sized cables transfer an estimated 97 percent of international communication.[13] In addition to carrying electronic mail, submarine cables transmit information that is necessary to carry out almost every facet of modern life, such as accessing social media data, streaming live video, or transmitting financial transactions.[14] This ability to share data globally via undersea telecommunications infrastructure is vital during moments of international crisis, such as a global pandemic with little thought on how much society relies on this network of fiber-optic garden hoses on the ocean floor. Thus, the targeting of just a few of these submarine cables, especially

---

[10] David Alexander, *U.S. Reserves Right to Meet Cyber Attack with Force*, REUTERS (Nov. 15, 2011, 7:48 PM), https://www.reuters.com/article/us-usa-defense-cybersecurity/u-s-reserves-right-to-meet-cyber-attack-with-force-idUSTRE7AF02Y20111116.

[11] Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land art. 54, Oct. 18, 1907, 36 Stat. 2277 [hereinafter 1907 Hague Regulations].

[12] *Id.*

[13] DOUGLAS BURNETT ET AL., SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 2 (2014). Although there are submarine cables that transmit electrical power, this article is primarily focused on submarine telecommunications cables.

[14] Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, 24 CATH. UNIV. J.L. & TECH 57, 58 (2015).

those connecting developing States and economies to the global marketplace, can have drastic and injurious consequences.

The fact that the security of submarine cables are threatened by both kinetic effects in the sea domain as well as cyber effects in the cyber domain is illustrative of the new reality that modern warfare no longer consists of lines on a battlefield.[15] The concept of "all-domain operations" combines the traditional domains of warfare (i.e., land, sea, and air) with "space, cyber, deterrent, transportation, electromagnetic spectrum operations, missile defense—all of these global capabilities together . . . to compete with a global competitor and at all levels of conflict."[16] To keep pace with battlefield realities and emerging concepts related to the use of force, LOAC must reflect modern warfare.

The current LOAC approach focuses on domain warfare, such as the laws of land, naval, air and missile, cyber, and space warfare. However, the Russian *Losharik* is an example of how advanced technologies can threaten multiple domains. In 2018, the Chairman of the Joint Chiefs of Staff wrote that "[w]hile the fundamental nature of war has not changed, the pace of change and modern technology, coupled with shifts in the nature of geopolitical competition, have altered the character of war in the 21st century."[17] As the character of warfare has changed, so too have the effects of destroying objects that have historically been lawfully targeted, such as submarine cables. The targeting of submarine cables is illustrative of how modern warfare—specifically all-domain operations—has outpaced the ability of LOAC to adequately protect critical civilian infrastructure. To thoroughly understand the legal issues related to targeting submarine cables, one must not simply apply a single-domain LOAC framework (e.g., the law of naval warfare for operations in the sea domain), but rather take an all-domain approach and analyze the target under (or at least consider

---

[15] Aaron Mehta, *'No Lines on the Battlefield': Pentagon's New War-Fighting Concept Takes Shape*, DEF. NEWS (Aug. 14, 2020), https://www.defensenews.com/pentagon/2020/08/14/no-lines-on-the-battlefield-the-pentagons-new-warfighting-concept-takes-shape.

[16] Colin Clark, *Gen. Hyten on the New American Way of War: All-Domain Operations*, BREAKING DEF. (Feb. 18, 2020, 7:01 AM), https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations.

[17] General Joseph F. Dunford Jr., *The Character of War and Strategic Landscape Have Changed*, 89 JOINT FORCES Q., no. 2, 2018, at 2.

the relevance of) the laws applicable to military operations in the cyber domain as well.

Upon considering the civilian population's reliance on submarine cables and the modern threat during armed conflict, it is clear that current LOAC rules and interpretations are unsatisfactory when applied to the targeting of submarine cables. Therefore, taking feasible precautions[18] during all-domain operations and mitigating harm to civilians in the cyber age requires adopting a new approach to LOAC. One approach, which is arguably the simplest, is to recognize "data" as an "object." This approach, however, has far-reaching consequences beyond the protection of submarine cables. A second, more targeted approach is to develop a special legal regime designed to protect the tangible networks that transfer data, such as submarine cables. This article focuses on the development of a new legal regime.[19]

This article explores a *lex ferenda* [20] that places submarine communication cables under special protection in the event of armed conflict.[21] Moreover, it focuses on the *jus in bello* targeting of submarine cables and presupposes that the intentional destruction of a submarine cable during peacetime, especially by a State's armed force, constitutes a belligerent act justifying the use of force in self-defense under the United Nations Charter and *jus ad bellum* principles.[22] Part II provides background on the development and use of submarine cables and their importance within today's global economic and social order. Part III presents a brief overview of the international legal regime that protects submarine cables in peacetime,

---

[18] "Combatants must take feasible precautions in planning and conducting attacks to reduce the risk of harm to civilians and other persons and objects protected from being made the object of attack." LAW OF WAR MANUAL, *supra* note 6, § 5.11.

[19] Whether the LOAC should consider "data" a type of "object" is a complex issue deserving extensive research and analysis. How the LOAC principles of distinction and proportionality would apply to the specific data transmitted through submarine cables is outside the scope of this article.

[20] *Lex Ferenda*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining the term as "law proposed for enactment").

[21] This article will not discuss whether hacking or some other form of interference with submarine cables in wartime violates international law.

[22] *See* INT'L INST. OF HUMANITARIAN L., SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Lousie Doswald-Beck ed., 1994), *reprinted in* 309 INT'L COMM. RED CROSS 595 (1995). Paragraph 60 of the *San Remo Manual* lists various belligerent acts that would render enemy merchant vessels military objectives, one of which is cutting undersea cables. *Id.* at 640.

while Part IV examines the current threat to submarine cables. Part V evaluates the *lex lata* (the law as it exists)[23] of targeting submarine cables in naval warfare and introduces the precedent of targeting them during naval operations in past conflicts. Given that targeting submarine cables achieves military effects across domains, Part VI presents the issue of targeting submarine cables in the cyber warfare context. Finally, Part VII provides recommendations on how to ensure the protection of submarine cables. Before examining the relevant legal regimes and LOAC principles, a brief recitation of the history of submarine cables helps to illuminate the issues.

II. Development and Use of Submarine Cables

"The United Nations, in 2010, described submarine cables as 'critical communications infrastructure' and 'vitally important to the global economy and the national security of all States.'"[24] Having a basic understanding of the development of this technology is critical to understanding its unique importance to the global economic and social order and the impact on the civilian population.

Halfway between the United States and the United Kingdom, in the middle of the Atlantic Ocean, U.S. and U.K. warships made history on 29 July 1858 when they spliced together two ends of copper cable and dropped it to the seafloor.[25] Eighteen days later, Queen Victoria and President James Buchannan would exchange telegrams.[26] What would have likely taken weeks or months to transmit by ship took only 17 hours and 40 minutes via cable.[27] While the cable would last only a few days, it "marked the first step in a communications revolution that would lead, ultimately, to the creation of the internet."[28] After Alexander Graham Bell's invention of the telephone in 1875 and the discovery of polyethylene[29] in 1933, a suitably protected submarine cable could carry more than one voice channel.[30] In

---

[23] *Lex Lata*, BLACK'S LAW DICTIONARY (11th ed. 2019).
[24] Davenport, *supra* note 14, at 62.
[25] SUNAK, *supra* note 1, at 12.
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] Polyethylene is a light, synthetic resin that forms the most widely used plastic in the world and can be modified to take on the properties of rubber. *Polyethylene*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/science/polyethylene (last visited Aug. 6, 2021).
[30] LIONEL CARTER ET AL., SUBMARINE CABLES AND THE OCEANS: CONNECT THE WORLD 14 (2009).

1956, two newly laid submarine cables between the United Kingdom and Newfoundland transmitted 707 calls between London and North America on their first day in use.[31]

With the advent of satellite communications technology in the 1970s and the 1980s, the transmission of a majority of international telecommunications was through space rather than through the century-old copper submarine cables then in existence.[32] However, the development of fiber optic technology would change the balance, and, in 1988, the first trans-oceanic fiber optic cable was put in service.[33] Since their employment, submarine cables have "outperform[ed] satellites in terms of the volume, speed, and economics of data and voice communications."[34]

There are now close to 448 submarine cables[35] grouped into more than 200 independent cable systems owned by a number of international consortiums, each consisting of anywhere between 4 and 30 private companies.[36] A single submarine cable consists of six to twenty-four hair-like, glass fiber optic wires.[37] Each wire can transmit 400 gigabytes of data per second via wavelengths of light that travel about 180,000 miles per second.[38] About the diameter of a garden hose,[39] submarine cables transmit approximately 97 percent of international communication.[40] The "backbone of the global economy,"[41] submarine cables provide the means to exchange more than 10 trillion U.S. dollars in daily transactions,[42] and they transmit millions of financial messages to over 8,300 banks and securities institutions

---

[31] *Id.*
[32] *Id.* at 15.
[33] *Id.* at 16.
[34] *Id.* at 15–16.
[35] Carl Schreck, *Explainer: How Vulnerable Are Undersea Cables That U.S. Says Russia Is Tracking?*, RADIO FREE EUR. (June 12, 2018, 4:44 PM), https://www.rferl.org/a/explainer-undersea-cables-u-s-says-russia-vulnerable-internet/29287432.html.
[36] INT'L SEABED AUTH., TECH. STUDY NO. 14, SUBMARINE CABLES AND DEEP SEABED MINING 17 (2015).
[37] Davenport, *supra* note 14.
[38] SUNAK, *supra* note 1, at 14.
[39] See *infra* app. A, for a photograph that depicts the size of modern cables; see *infra* app. B, for a map of active and planned cable networks with their associated cable landing stations.
[40] BURNETT ET AL., *supra* note 13.
[41] INT'L SEABED AUTH., *supra* note 36.
[42] Davenport, *supra* note 14, at 6 (quoting MICHAEL SECHRIST, NEW THREATS, OLD TECHNOLOGY 9 (2012).

in more than 200 countries.[43] Given the heavy reliance on submarine cables in the global marketplace, "[t]hese international connections over fiber-optic cables mean that cable disruptions can potentially affect multiple countries and lead to cascading issues internationally . . . ."[44]

From a U.S. defense perspective, submarine cables are a vital link to U.S. forces, as well as U.S. allies and partners, overseas. In fact, the U.S. Department of Defense (DoD) relies on commercially owned submarine cables to transmit 95 percent of its international communications.[45] For example, the DoD has used submarine cables to stream live video data captured by unmanned aerial vehicles above the battlefields of Iraq and Afghanistan to command centers at home.[46] The DoD also uses submarine cables to control the battlespace by transmitting data that is then collected, processed, stored, disseminated, and managed via the Global Information Grid.[47] Given the DoD's reliance on commercial submarine cables, protection of this undersea network during armed conflict is critical because, "without ensured cable connectivity, the future of modern warfare is in jeopardy."[48]

III. Status of Submarine Cables Under International Law

The oldest international convention currently in force and dedicated to the protection of submarine cables is the 1884 Convention for the Protection of Submarine Telegraph Cables (1884 Convention).[49] "The 1884 Cable Convention is a stand-alone convention dealing solely with the *protection* of submarine telegraph cables."[50] Its primary purpose is to require signatory States to adopt domestic legislation that criminalizes the destruction of

---

[43] JAMES DEAN ET AL., THREATS TO UNDERSEA CABLE COMMUNICATIONS 11 (2017).
[44] *Id.*
[45] Hinck, *supra* note 5.
[46] Brian Mockenhaupt, *We've Seen the Future, and It's Unmanned*, ESQUIRE (Oct. 14, 2009), https://www.esquire.com/news-politics/a6379/unmanned-aircraft-1109.
[47] *Global Information Grid*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/global_information_grid (last visited Aug. 6, 2021) (defining the Global Information Grid as "[t]he globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.").
[48] MICHAEL SECHRIST, CYBERSPACE IN DEEP WATER 5 (2010).
[49] Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 24 Stat. 989 [hereinafter 1884 Convention].
[50] Davenport, *supra* note 14, at 67.

submarine cables.[51] Forty States are a party to the 1884 Convention, including the United States and Russia.[52] Although Article X permits warships to visit and board other ships suspected of tampering with submarine cables, the 1884 Convention does not apply in armed conflict, and it expressly prohibits the boarding of warships of other States.[53]

Moreover, while the 1884 Convention is the only treaty solely dedicated to the protection of submarine communications cables, other legal conventions also include provisions that relate to submarine cables. First, in the 1958 Geneva Conventions on the High Seas and the Conventional Shelf, the international community "secured the legal principle that [S]tates could not obstruct the construction of undersea cables in international waters."[54] In 1982, the Third United Nations Convention on the Law of the Sea (UNCLOS), which superseded the 1958 Geneva Convention for signatory States, expanded submarine cable protections as part of a comprehensive and monumental effort to develop the "constitution for the oceans."[55] Of the 320 articles and 9 annexes, 6 articles address submarine cables. Article 113 essentially restates Article II of the 1884 Convention, requiring States to "adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence . . . shall be a punishable offence."[56] Unlike the 1884 Convention, however, UNCLOS "stops short of giving warships the right to board a vessel suspected of intentionally trying to damage undersea cables in international waters, making it difficult for naval powers to effectively deter hostile vessels."[57] In addition to criminalizing injury to submarine

[51] 1884 Convention, *supra* note 49, 24 Stat. at 993 ("The breaking or injury of a submarine cable, done willfully or through culpable negligence, and resulting in the total or partial interruption or embarrassment of telegraphic communication, shall be a punishable offense, but the punishment inflicted shall be no bar to a civil action for damages.").
[52] Davenport, *supra* note 14, at 67 (citing BURNETT ET AL., *supra* note 13, at 64).
[53] 1884 Convention, *supra* note 49, 24 Stat. at 997 ("It is understood that the stipulations of this Convention shall in no wise affect the liberty of action of belligerents.").
[54] SUNAK, *supra* note 1, at 16.
[55] Davenport, *supra* note 14, at 67.
[56] United Nations Convention on the Law of the Sea art. 113, Dec. 10, 1982, 1833 U.N.T.S. 397.
[57] SUNAK, *supra* note 1, at 17.

cables, UNCLOS protects States' "*freedom to lay, repair and maintain*" submarine cables while balancing the rights of coastal States.[58]

IV. The Threat to Submarine Cables

"Cables are inherently vulnerable as: their location is generally publicly available [so as to mitigate accidental damage by fishermen, etc.], they tend to be highly concentrated geographically both at sea and on land, and it requires limited technical expertise and resources to damage them."[59] While anchors and dredging equipment can accidently sever submarine cables, some of the Russian Navy's submarines can exploit these vulnerabilities while operating on the high seas and outside State jurisdiction.[60] In addition to deep-sea nuclear submarines like the *Losharik*, Russia also deploys a *Yantar*-class intelligence vessel that has the capability to carry two smaller submarines, which some commentators believe are designed to cut or hack submarine cables.[61] In 2015, the *Yantar* was discovered probing a cable route during its voyage to Cuba, resulting in reports that the Russians were targeting highly classified DoD-owned submarine cables connecting the naval base at Guantanamo Bay with Miami.[62] The suspicion that Russia is actively exercising the ability to target submarine cables has provoked strong responses from U.S. national security leaders. In 2017, Admiral Michelle Howard, who at the time was serving as the commander of U.S. Naval Forces Europe, stated that "[w]e're seeing activity [by Russia] that we didn't even see when it was the Soviet Union. . . . [T]he activity in this theatre has substantially moved up in the last couple of years."[63] Furthermore, Admiral James Stavridis, who retired in 2013 as the Supreme Allied Commander Europe, has opined that Russia's relative weakness, when matched with conventional forces of the North Atlantic Treaty Organization, "raises the appeal of asymmetric targets like fibre-optic cables."[64]

---

[58] Davenport, *supra* note 14, at 68.
[59] SUNAK, *supra* note 1, at 19.
[60] *See* Ma & Pickrell, *supra* note 2.
[61] SUNAK, *supra* note 1, at 30.
[62] Hinck, *supra* note 5.
[63] Andrea Shalal, *Russian Naval Activity in Europe Exceeds Cold War Levels—U.S. Admiral*, REUTERS (Apr. 9, 2017, 10:54 AM), https://www.reuters.com/article/usa-russia-military-idINKBN17B0OA.
[64] Stavridis, *supra* note 1, at 10.

In addition to voicing concerns, other departments in the U.S. Government have taken substantive action. In 2018, for example, the U.S. Treasury Department sanctioned five Russian firms and three Russian nationals alleged to have provided support to Russia's primary security agency, the Federal Security Service, in tracking underwater fiber-optic cables.[65] In support of the Treasury Department's sanctions, Congressman Jim Langevein, who serves as a member of both the House Armed Services and House Homeland Security Committees, stated that, "[w]ere those [cables] ever to be cut, there would be significant damage to our economy and to our everyday lives."[66] In addition to having the capability, Russia has also shown a willingness to destroy access to data in armed conflict. During the annexation of Crimea in 2014, one of Russia's first acts was to disrupt internet connectivity to the Crimean peninsula and isolate it from the rest of Europe.[67]

Given that Russia has the technological capability in its deep-sea submersibles and intelligence ships to attack submarine cables, as well as the willingness to do so, as shown during its invasion of Crimea, the threat to submarine cables is real. If coordinated attacks against multiple submarine cables were to occur at the outbreak of armed conflict, there would likely be a catastrophic impact on not only the targeted belligerent, but also the global economic and social order as a whole. The question then becomes whether submarine cables are lawful targets under the current LOAC rules and interpretations.

V. The Law of Naval Warfare and Submarine Cables

The issue of whether submarine cables are legitimate targets during armed conflict is a historical one.

> The issue was raised regularly in the nineteenth century—from an 1864 draft treaty among France, Brazil, and others,

---

[65] Morgan Chalfant & Olivia Beavers, *Spotlight Falls on Russian Threat to Undersea Cables*, THE HILL (June 17, 2018, 8:14 PM), https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables.

[66] *Id.*

[67] Damien Sharkov, *Russian Ships Could Cause 'Catastrophe' for West by Cutting Transatlantic Internet Cables*, NEWSWEEK (Dec. 15, 2017, 5:08 AM), https://www.newsweek.com/russian-forces-could-cause-catastrophe-west-cutting-internet-cables-749047.

> to the 1874 Brussels conference on the laws of war, to the 1879 meeting of the Institut de Droit International (IDI) and the 1882 Conference for the Protection of Submarine Cables. But cable neutralization was not achieved.[68]

Despite the recognition of their importance to the global economic and social order and the multiple legal regimes in force to protect them in peacetime, efforts to examine their status in armed conflict is almost non-existent. In fact, the primary legal handbook on submarine cables "notes the potential risk of terrorist attacks, but says surprisingly little about the threat of war."[69]

The status of submarine cables in armed conflict may receive such little attention because State action and a traditional application of LOAC suggest that the matter is settled. After all, as historical precedent has shown, belligerents have targeted submarine cables since the technology's inception. However, if advances in technology have perpetuated the evolution of all-domain warfare and changed the character of war, it begs the question of whether the status of this undersea technology as a legitimate target should also change. "In our world so dependent on internet interconnectivity, States have still not agreed to protect submarine cables from the putative rights of belligerents."[70]

This part will explore the relevant *lex lata* of targeting submarine cables. Despite explicit language that destruction of submarine cables in armed conflict is to be prohibited or avoided, historical precedent has clearly exploited the caveats and exceptions included in the restatements discussed below, rendering the current rules weak in their ability to protect such a vital component of the global economic and social order.[71]

---

[68] Douglas Howland, *The Limits of International Agreement: Belligerent Rights vs. Submarine Cable Security in the Nineteenth Century*, 2 JUS GENTIUM: J. INT'L LEGAL HIST. 67, 71 (2017).
[69] *Id.* at 92.
[70] *Id.*
[71] *See* James Kraska, *Submarine Cables in the Law of Naval Warfare*, LAWFARE (July 10, 2020, 8:01 AM), https://www.lawfareblog.com/submarine-cables-law-naval-warfare.

A. *Lex Lata* of Submarine Cables in the Law of Naval Warfare

Before reviewing the history of targeting submarine cables in wartime, it is informative to review the *lex lata* related to the protection of submarine cables. The only LOAC legal instrument that relates specifically to submarine cables is Article 54 of the 1907 Hague Regulations.[72] Article 54, however, only applies to submarine cables connecting occupied territory with neutral territory. Therefore, to obtain some clarity regarding the legal status of submarine cables in wartime, one must look to the various restatements. This section provides a brief review of the three primary, non-binding legal treatises related to submarine cables and the laws of naval warfare.

1. Oxford Manual of the Laws of Naval Warfare *(1913)*

Under Article 54, the *Oxford Manual of the Laws of Naval Warfare* suggests that the rules governing the destruction of submarine cables during wartime fall under a binary analytical framework: (1) status of the States connected by cables and (2) jurisdiction pertaining to the maritime zone where the cables are targeted.[73] The special committee reinforced the consensus that cables connecting belligerents or two points within a belligerent State are lawful targets. Additionally, with regard to cables connecting belligerents with neutral States, the special committee wrote that these cables may also be destroyed, but it is unlawful to destroy a cable in the waters of the neutral State. "On the high seas," however, Article 54 C states, "this cable may not be seized or destroyed unless there exists an effective blockade and within the limits of that blockade, on consideration of the restoration of the cable in the shortest time possible."[74] Finally, the special committee stated that "[s]eizure or destruction may never take place except in case of absolute necessity."[75]

---

[72] 1907 Hague Regulations, *supra* note 11.
[73] INST. OF INT'L LAW, THE LAWS OF NAVAL WARFARE GOVERNING THE RELATIONS BETWEEN BELLIGERENTS art. 54 (1913), *reprinted in* THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 857 (Dietrich Schindler & Jiří Toman eds., 1988).
[74] *Id.*
[75] *Id.*

2. San Remo Manual on International Law Applicable to Armed Conflicts at Sea *(1994)*

Prepared by a group of "legal and naval experts . . . . [t]he purpose of the [*San Remo*] *Manual* is to provide a contemporary restatement of international law applicable to armed conflicts at sea."[76] Within the *San Remo Manual*, the only rule that explicitly relates to submarine cables is paragraph 37, which states: "Belligerents shall take care to avoid damage to cables and pipelines laid on the sea-bed which do not exclusively serve the belligerent."[77] While recognizing the "concern for protection of cables," the explanation to paragraph 37 acknowledges "that cables or pipelines exclusively serving one or more of the belligerents might be legitimate military objectives."[78]

3. Oslo Manual on Select Topics of the Law of Armed Conflict *(2020)*

Funded by the Norwegian Ministry of Defense, a group of experts convened in Oslo in 2015 to address the gaps created by advancements in technology and military concepts since the 2009 Program on Humanitarian Policy and Conflict Research's *Manual on International Law Applicable to Air and Missile Warfare*.[79] The group of experts restated the rule that "[s]x."[80] The caveat "unless they qualify as lawful targets" creates sufficient ambiguity to render the rule essentially worthless. Additionally, the commentary to Rule 69 notes that, although

> Article 54 of the 1907 Hague Regulations and the provisions of the *San Remo Manual* seem to reflect correctly the *lex lata* insofar as submarine pipelines and submarine high voltage cables are concerned. . . . [i]t is, however, doubtful whether the 1907 Hague Regulations and the *San Remo* provisions also apply to submarine communications cables.[81]

---

[76] INT'L INST. OF HUMANITARIAN L., SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA 5 (Lousie Doswald-Beck ed., 1994).
[77] *Id.* at 111.
[78] *Id.*
[79] OSLO MANUAL ON SELECT TOPICS OF THE LAW OF ARMED CONFLICT: RULES AND COMMENTARY, at v–vi (Yoram Dinstein & Arne Willy Dahl eds., 2020).
[80] *Id.* at 63.
[81] *Id.*

The international legal experts in Oslo recognized how technological advances have changed the character of the effects related to targeting submarine cables. They stated that "other than telegraphic cables, modern submarine communications cables are the backbone of global data traffic. . . . Accordingly, it is important to distinguish between submarine communications cables and other submarine cables."[82] That distinction, however, is neither required under any sort of legal framework nor apparent in the history of naval warfare and the activities of modern navies.

B. Historical Precedent

Given the utility of telegraph cables for military operations in wartime, the status of submarine cables in armed conflict has been a topic of discussion since their inception.

> [A]s the submarine cable network developed, the question of its destruction in warfare was present from the start. The conferences and discussions about cable security between 1864 and 1907 demonstrate that the great powers, leading statesmen, and international lawyers were arguably committed to making the world an environment safer for war.[83]

The first and only expressed prohibition of targeting submarine cables in wartime was included in the 1864 draft treaty between France, Brazil, Haiti, Italy, and Portugal.[84] The treaty, however, was suspended in 1872 because the cable was never laid.[85] Additionally, just prior to the Franco-Prussian War, the United States intended to host an international convention in Washington to resolve the issue of submarine cables during wartime.[86] Because the conflict raging in Europe at the time consumed the U.S. Government and other States, the convention never occurred. Historians suggest that had the convention taken place in Washington, it likely would have concluded that targeting cables during wartime amounted to an act of

---

[82] *Id.*
[83] Howland, *supra* note 68, at 70.
[84] BURNETT ET AL., *supra* note 13, at 66.
[85] Howland, *supra* note 68, at 78.
[86] R. J. R. Goffin, *Submarine Cables in Time of War*, 15 L.Q. REV. 145, 146 (1899).

piracy, and it may have developed a legal instrument to prohibit the targeting of international telecommunications in war and in peace.[87]

More than a century before the tragic deaths of the Russian sailors in July 2019, the U.S. Navy was targeting submarine cables in their maritime operations. On 24 May 1898, readers of the *New York Times* awoke to the headline "*Right to Cut Cables in War; Admiral Dewey Created a New Precedent Under the Law of Nations in Manila Bay*."[88] At the time, U.S naval forces were engaged in fleet operations against the Spanish Armada in the Philippines during the Spanish-American War. In order to degrade the command and control of the Spanish fleet, Admiral Dewey ordered the submarine telecommunications cables linking the Philippines with Hong Kong (and thus the rest of the world) be cut. As the *New York Times* declared, Admiral Dewey established international legal precedent on that day in Manila Bay. Even though submarine cables were legitimate targets at the time, many believed that "a belligerent was obliged to recompense the damage when peace was restored."[89] When the U.S. Government refused to indemnify the British owner of the cable, diplomats and international legal experts grew concerned.[90] As a result, during the fourth Hague Peace Convention in 1907, drafters included a section that required compensation to the cable owner and permitted the seizure or destruction of submarine cables in neutral waters only under the condition of absolute necessity.[91]

Both World Wars also supported the case that submarine cables were lawful targets. At the outbreak of World War I, Britain targeted Germany's submarine cables, and Germany retaliated by targeting Britain's cables in the Pacific and Indian Oceans in an attempt to isolate London from its colonies outside Europe.[92] The same activity also occurred during World War II. For example, during Operation Sabre, an Australian Navy midget

---

[87] *Id.*

[88] *Right to Cut Cables in War: Admiral Dewey Created a New Precedent Under the Law of Nations in Manila Bay*, N.Y TIMES, May 24, 1898, at 2; *see* Jonathan Reed Winkler, *Silencing the Enemy: Cable-Cutting in the Spanish-American War*, WAR ON THE ROCKS (Nov. 6, 2015), https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war.

[89] Howland, *supra* note 68, at 72.

[90] *Id.*

[91] *Id.*

[92] Davenport, *supra* note 14, at 80; *see also* Mark Stout, *Trans-Atlantic Bandwidth: Then and Now*, WAR ON THE ROCKS (Oct. 30, 2015). https://warontherocks.com/2015/10/trans-atlantic-bandwidth-then-and-now.

submarine cut the undersea cable linking Singapore with Saigon, forcing the Japanese to send messages via encrypted radio signal that the Allies had decoded earlier in the war.[93]

More recently, when Russia invaded Ukraine's Crimean Peninsula, one of its first acts at the outbreak of the conflict was to target Crimea's internet. "According a 2016 Chatham House report, during the 2014 invasion of Crimea, Russian forces seized the peninsula's main internet traffic exchange point, isolating Crimea's internet from the rest of the world at a key moment in the conflict."[94]

Although the history shows multiple attempts to protect submarine cables, State practice has consistently been to target the cables in wartime and exploit the "liberty of action of belligerents"[95] exception in the 1884 Convention. If navies were to apply current LOAC rules and interpretations today, despite the change in technology and their impact to the civilian population, the analysis suggests that submarine cables would remain lawful targets.

VI. The Law of Cyber Warfare and Submarine Cables

Despite the fact that the binding rules found in the 1907 Hague Regulations and the non-binding restatements of the *Oxford, San Remo*, and *Oslo Manuals* suggest that submarine cables are protected during armed conflict, an analysis under an Industrial Age, single-domain application of LOAC rules suggests otherwise. To reconcile this inconsistency, the development of legally binding protections must be considered. Before exploring possible ways to ensure that submarine cables are protected during armed conflict, it is worth exploring the matter through the context of international law as applied to cyber warfare.

Two fundamental issues arise when discussing whether a single-domain approach to applying LOAC principles or Industrial Age LOAC treaties sufficiently apply in the cyber age: (1) which objects should be protected if

---

[93] *Operation Sabre Helps End War in the Pacific*, AUSTL. GOV'T: DEP'T OF VETERANS' AFFS., https://anzacportal.dva.gov.au/stories-service/australians-war-stories/operation-sabre-helps-end-war-pacific (June 3, 2019).
[94] Hinck, *supra* note 5.
[95] 1884 Convention, *supra* note 49, 24 Stat. at 997 ("It is understood that the stipulations of this Convention shall in no wise affect the liberty of action of belligerents.").

the LOAC principles of distinction and proportionality are meant to mitigate harm to the civilian population, and (2) whether the law that currently exists can adequately protect those objects. The view of a majority of experts that produced the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, a comprehensive treatise discussed further below, is that LOAC protects tangible objects but not intangible ones (e.g., data).[96] In the cyber age, this interpretation fails to fulfill the legal obligation to mitigate harm to the civilian population. Just as it is impossible to separate the ship from the sea, it is illogical to distinguish the intangible data from the tangible networks it traverses when applying LOAC to cyber operations. The physical layers of cyberspace are insignificant without the invisible data that flows through it. As evidenced in the scholarship related to LOAC in cyber warfare, the primary issue to settle is how to mitigate harm to the civilian population from the non-kinetic, intangible effects that modern military capabilities are able to achieve. Moreover, the issue of protecting submarine cables is similar in that the same non-kinetic, intangible effects are achieved through a method of warfare as old as the late nineteenth century's Spanish-American War.

It is the impact on the non-kinetic, intangible objects (e.g., data, economy, society) that make the destruction of submarine cables so costly—the so called "knock-on" effects.[97] The reason that their destruction has such economic and social impact is not because of what they are, but because of what they transmit. Under current LOAC rules and interpretations, the targeting of a bridge or railway, even if used by civilians, is permissive so long as there is a clear military advantage, such as the prevention of the transportation of weapons or troops.[98] The bridge or railway would have likely been targeted, despite the fact that it also carried civilians to jobs or goods to markets, upon both of which the civilian population depends. Under a traditional proportionality analysis, although the potential of death

---

[96] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 437 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL].

[97] Commander Peter Pascucci, *Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, 26 MINNESOTA J. INT'L L. 419, 449–51 (2017).

[98] *Cf.* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 56, June 8, 1977, 1125 U.N.T.S. 3 (prohibiting attacks on dams, dykes, and nuclear electrical generating stations because they contain dangerous forces and not because of their utility to the civilian population). Although 168 States have ratified Additional Protocol I, the United States has not. *See* LAW OF WAR MANUAL, *supra* note 6, § 5.13.1.

or injury to those civilians (and possibly the nature of the goods, such as medicine for sick noncombatants) is considered, international law currently ignores the intangible forces associated with the movement of the people and goods on that same bridge or road. For example, these intangible forces could include the skill of the civilian worker and his income or the impact the goods have on the health and welfare of the local village. Because these forces are impossible to calculate accurately and thus impractical to consider in a proportionality analysis, it traditionally has been prudent to focus only on quantitative factors, such as the civilian casualty count or the economic cost to the enemy's war effort when destroying or damaging a civilian object. Additionally, these forces usually only have a local or isolated effect, thus permitting their destruction to have minimal value in the context of an armed conflict.

In the cyber age, it has become more difficult to ignore the effects that the intangible forces, specifically data and its disruption, have on the civilian population as a whole. Where the global economic and social order of the Industrial Age depended on tangible networks (such as roads, bridges, railways, and ships) to carry tangible goods, people in the cyber age depend on the intangible as well. Unlike any time in history, the global economic and social order now relies on the expedient and uninterrupted transfer of data. Therefore, the issue raised in this new cyber age is whether an application of LOAC should recognize and protect the intangible as it has the tangible.

The international group of experts addressed this issue briefly in the *Tallinn Manual*. A majority maintained the view that, under existing law, "data is intangible and therefore neither falls within the 'ordinary meaning' of the term object . . . [t]herefore an attack on data *per se* does not qualify as an attack."[99] A minority of the experts, however, believed that certain civilian datasets should be protected from targeting, such as "social security data, tax records, and bank accounts," deletion of which "run[s] counter to the principle (reflected in Article 48 of Additional Protocol I) that the civilian population enjoys general protection from the effects of hostilities."[100] Whereas the classification of "data" under LOAC

[99] TALLINN MANUAL, *supra* note 96.

[100] *Id.* While the United States has not ratified Additional Protocol I, its position is that article 48 reflects customary international law. *See* COLONEL THEODORE T. RICHARD, UNOFFICIAL UNITED STATES GUIDE TO THE FIRST ADDITIONAL PROTOCOL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 83 (2019).

may be debatable, there is a consensus of how critical data is to the civilian population in the cyber age.

A. Applying *Jus in Bello* Principles to Targeting Submarine Cables in the Cyber Age

According to the *Tallinn Manual*, there are two "cardinal" principles of LOAC: the prohibition of unnecessary suffering and distinction.[101] From the principle of *distinction*, LOAC requires that if there is likely to be civilian collateral damage when targeting a military objective, the impact to the civilian person or object must be *proportional*.

1. Distinction

Rule 93 of the *Tallinn Manual* states that "the principle of distinction applies to cyber-attacks," requiring belligerents at all times to distinguish between civilian objects and military objectives.[102] The 1868 Saint Petersburg Declaration first articulated this rule, which was later adopted in Article 52(1) of Additional Protocol I,[103] stating in part that "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy."[104] The *Tallinn Manual* applies this rule to the cyber domain and states, "[c]ivilian objects shall not be made the object of cyber-attacks. Cyber infrastructure may only be made the object of attack if it qualifies as a military objective."[105]

As described above, both civilians and militaries use commercially owned submarine cables to transfer data between continents. "As a matter of law, status as a civilian object and military objective cannot coexist; an object is either one or the other. This principle confirms that all dual-use

---

[101] *Compare* RICHARD, *supra* note 100, at 420, *with* LAW OF WAR MANUAL, *supra* note 6, § 2.1. "Three interdependent principles—*military necessity*, *humanity*, and *honor*—provide the foundation for other law of war principles, such as *proportionality* and *distinction*, and most of the treaty and customary rules of the law of war." LAW OF WAR MANUAL, *supra* note 6, § 2.1.

[102] TALLINN MANUAL, *supra* note 96, at 420.

[103] While the United States has not ratified Additional Protocol I, its position is that article 52(1) reflects, in part, customary international law. The United States does, however, object to the rule holding that civilian objects shall not be the object of reprisals. *See* RICHARD, *supra* note 100, at 98 n.107.

[104] TALLINN MANUAL, *supra* note 96, at 434.

[105] *Id.*

objects and facilities are military objectives, without qualification."[106] The *Tallinn Manual*'s experts used the analogy of a road network to illustrate how the dual-use principle applies in the cyber domain. If belligerents use a bridge to transport materiel to the front line while the local civilian population also uses it for going about their everyday lives, it is a valid military objective because of its military use. The principle supports the conclusion that "so long as it is reasonably likely that a road in the network may be used, the network is a military objective subject to attack. There is no reason to treat computer networks differently."[107]

Therefore, under a traditional application of the dual-use principle, where civilians and militaries use submarine cables simultaneously, they are military objectives. Even though an object that is otherwise used primarily by civilians is a lawful target because its nature, location, purpose, or use makes an effective contribution to military action,[108] "it will be appropriate to consider in applying the principle of proportionality the harm to the civilian population that is expected to result from the attack on such a military objective."[109]

Another key issue raised by the principle of distinction is the positive obligation of States to keep their military objectives separate from civilians and civilian objects. "*Distinction* also creates obligations for parties to a conflict to take feasible measures to separate physically their own military objectives from the civilian population and other protected persons and objects."[110] Therefore, under current LOAC rules and interpretations, it may be necessary for militaries to refrain from utilizing submarine cables to transfer military related data during armed conflict in order to avoid harm to the civilian population. As stated above, the DoD currently uses commercial submarine cables to transmit 95 percent of its international communications.[111] By applying the traditional LOAC principle of distinction, without specific legal agreements to protect submarine cables in wartime, the DoD's ability to communicate with its forces overseas would collapse. Additionally, given that most States do not have the capacity or capability to lay government-owned cables for the exclusive use of their

---

[106] *Id.* at 446; *see* LAW OF WAR MANUAL, *supra* note 6, § 5.6.1.2.
[107] TALLINN MANUAL, *supra* note 96, at 446.
[108] *See* LAW OF WAR MANUAL, *supra* note 6, § 5.6.6.
[109] *Id.* § 5.6.1.2.
[110] *Id.* § 2.5.3.2.
[111] Hinck, *supra* note 5.

military, the part of the distinction principle obligating States to separate their military objectives from civilian objects is not a practical option at this time.

2. Proportionality

If the targeting of military objectives would result in injury to civilians or damage to civilian objects, a proportionality analysis is required. As Rule 113 of the *Tallinn Manual* states, "[a] cyber-attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited."[112] First, it is critical to understand that "[i]n war, incidental damage to the civilian population and civilian objects is unfortunate and tragic, but inevitable."[113] Therefore, the targeting of military objectives need not have zero impact to the civilian populations or its objects to be lawful.

Take, for example, a scenario in which Russia's navy, in support of a Middle East ally, targets five of the six cables located in the Mediterranean Sea that connect Egypt with Europe. A repaired *Losharik* would likely either sever the cables in real time or place remote-controlled explosives on the cables prior to the outbreak of the conflict. While the destruction of the cables themselves would cost the cable owner only a few hundred thousand dollars to repair, the incidental impacts would be much more costly. Egyptian internet capacity would degrade by 70 percent.[114] Further, because India heavily relies on the same five cables for 50 to 60 percent of its internet connectivity to Europe, the cutting would significantly affect their major economic outsourcing sector.[115] Despite the harm to Egypt's and India's civilian populations, both of which are neutral in the conflict, the primary purpose of targeting the cables would be degradation of the command and control capabilities of Russia's overseas enemy. By targeting the five submarine cables, their adversary's communications traffic to the region collapses and video streaming capacity degrades to a level that would require enemy commanders to decrease exponentially daily unmanned aerial vehicle flights that provide critical surveillance and kinetic strike

---

[112] TALLINN MANUAL, *supra* note 96, at 470.
[113] LAW OF WAR MANUAL, *supra* note 6, § 2.4.1.2.
[114] SUNAK, *supra* note 1, at 37 (recounting the 2008 destruction of five undersea cables that adversely affected Egypt's westbound internet connectivity).
[115] *Id.*

capabilities.[116] Regardless of the relatively low repair cost associated with the tangible damage to the cables, it would be unlikely, or at the very least extremely challenging, that a cable repair ship would be able to gain access and repair the cables within an area of active hostilities.

The incidental effects described above are not theoretical. In 2008, two merchant ships accidentally severed five submarine cables off the coast of Egypt, and the result was just as portrayed above.[117] Despite the far-reaching impact on the civilian population, whether Russia's targeting of the cables is lawful turns on whether the cutting is *excessive* when weighed against its military advantage. While there is no doubt that degrading a belligerent's ability to communicate with its forces overseas is advantageous, determining whether the collateral damage is *excessive* does not necessarily require the commander to calculate these difficult-to-measure incidental effects.

Although the term "excessive" is not defined in international law, the *Tallinn Manual*'s majority "took the position that extensive collateral damage may be legal if the anticipated concrete and direct military advantage is sufficiently great. Conversely, even slight damage may be unlawful if the military advantage expected is negligible."[118] The DoD offers additional guidance when attempting to determine whether damage would be excessive:

> Determining whether the expected incidental harm is excessive does not necessarily lend itself to quantitative analysis because the comparison is often between unlike quantities and values. The evaluation of expected incidental harm in relation to expected military advantage intrinsically involves both professional military judgments as well as moral and ethical judgments evaluating the risks to human life (e.g., civilians at risk from the attack, friendly forces or civilians at risk if the attack is not taken).[119]

---

[116] *Id.* at 21.
[117] *See id.* at 37 (providing several such examples).
[118] TALLINN MANUAL, *supra* note 96, at 473.
[119] LAW OF WAR MANUAL, *supra* note 6, § 5.12.3.

B. Submarine Cables in the *Tallinn Manual*

The status of submarine cable protections under the laws of cyber warfare has already been considered. Within its chapter on the law of the sea, the *Tallinn Manual* restates the freedoms of States regarding submarine cables established in UNCLOS.[120] It acknowledges that the "infliction of damage to cables by a State is prohibited as a matter of customary international law," but notes that the general rule is "without prejudice to the rules applicable during armed conflict."[121] Part IV of the *Tallinn Manual* covers how LOAC applies in the cyber domain, and it mentions submarine cables twice. Both times, the experts restate Article 54 of the 1907 Hague Regulations, which "provides that submarine cables connecting an occupied territory with neutral territory may be seized or destroyed 'in case of absolute necessity,' subject to the restoration and compensation after the end of war."[122]

Despite the direct economic and social harm to neutral States, the targeting of five garden-sized, fiber optic cables that cost a few hundred thousand dollars to repair[123] is minimal when compared to the degradation in the belligerent's command and control network. Thus, even if applying the *Tallinn* majority's interpretation of LOAC principles, the targeting of submarine cables remains lawful.

As shown above, applying a single-domain LOAC framework—using interpretations of LOAC principles and treaties developed in the Industrial Age—fails to satisfactorily protect necessary and critical civilian infrastructure during all-domain operations. A traditional interpretation of the LOAC principles (i.e., distinction and proportionality), treaty law developed in the Industrial Age, and State practice all suggest that targeting submarine cables remains lawful, despite the likely calamitous second and third order effects to the civilian population. However, if States (and their military lawyers) abandon the single-domain approach and instead view LOAC through an all-domain lens, gaps in legal protections, such as the targetability of submarine cables, may begin to be adequately addressed.

---

[120] TALLINN MANUAL, *supra* note 96, at 252.
[121] *Id.* at 256.
[122] *Id.* at 510, 551–52 (citing 1907 Hague Regulations, *supra* note 11).
[123] *See supra* Section VI.A.2.

VII. Protecting Submarine Cables in Modern Warfare

"The debate regarding whether [LOAC] applies to cyberspace is largely settled."[124] However, as the issue of targeting submarine cables illustrates, there are significant "deficiencies in the application of the principles of distinction and proportionality to cyberwar . . . ."[125] The lawfulness of naval operations are often viewed through a single-domain lens using LOAC principles that are "premised on a paradigm in which most of the deleterious consequences that [they seek] to temper are physically destructive or injurious."[126] However, when the operation seeks to achieve a cyber effect (e.g., targeting submarine cables), the result is that current LOAC rules and interpretations fall short of protecting the civilian population during all-domain operations. One solution is to develop a comprehensive LOAC regime for the cyber age, such as Additional Protocol IV.[127] This approach, however, comes with significant risks and is well outside the scope of this article. However, the overarching themes in such a discussion inform whether there should be a change to the law of naval warfare in order to place submarine cables under special protection during armed conflict.

Despite the historical precedent of targeting submarine cables in wartime, applying LOAC during all-domain operations should reflect how the evolution of technology has changed the ways in which civilian populations can be harmed or injured.[128] A severed telegraph cable may have had some local impact in Admiral Dewey's era, but it did not come close to the harm that the destruction of a submarine cable causes today. Therefore, to ensure that LOAC principles and rules in the cyber age provide adequate protections during all-domain operations, States must be obligated to protect submarine cables in wartime either through custom or treaty.

---

[124] Pascucci, *supra* note 97, at 451.
[125] *Id.*
[126] Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 289 (2014).
[127] *See generally* Pascucci, *supra* note 97.
[128] In the cyber age, disinformation can arguably be just as harmful to the civilian population as inaccessibility of data. While not the focus of this paper, perhaps the current LOAC principles and rules related to disinformation need to be re-examined given the potential modern effect.

A. 1884 Convention

The simplest remedy is to amend the 1884 Convention, which would require the consent of the thirty signatories. Although the amended 1884 Convention would not obligate non-signatory States, those States that have the technological and military capabilities to target cables in the high seas—mainly Russia and the United States—are signatories. If such a consensus could be reached, removing the language from Article XV ("shall in no wise affect the liberty of action of belligerents")[129] and explicitly declaring submarine cables unlawful targets in wartime would be sufficient to afford submarine cables special protection during armed conflict.

One State that did not sign the 1884 Convention and would thus be exempt from the amended treaty's prohibition of targeting submarine cables during armed conflict is the People's Republic of China. This is significant, given that State's growing blue-water naval capabilities. Moreover, because of China's exclusion under this approach, it would be far more effective to either develop a new treaty or articulate and defend a State practice that obligates all States that have the means, opportunity, and possible motive to target submarine cables in armed conflict.

B. New Convention on the Protection of Submarine Cables in Armed Conflict

Another approach is to initiate a stand-alone agreement that declares the importance of submarine cables to civilization and places them under special protection during wartime. While this approach requires the right geopolitical conditions just as much as it requires an acknowledgement of a legal necessity, the international community has made similar concessions before during periods of great power competition. The most analogous legal instrument designed to protect an object because of intangible effects is the 1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict, which placed "cultural property" under "special protection" in the event of armed conflict.[130]

Within the cornucopia of LOAC treaties and conventions that followed the Geneva Conventions, the convention to protect cultural property is

[129] 1884 Convention, *supra* note 49, 24 Stat. at 997.
[130] *See* Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, S. TREATY DOC. NO. 106-1, 249 U.N.T.S. at 240.

unique. Most post-Geneva treaties, such as the "Convention on Prohibitions or Restriction on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects" (and its progeny)[131] and the "Chemical Weapons Convention," were designed to prevent unnecessary suffering—one of the cardinal principles of LOAC.[132] In the case of cultural property, however, destroying an ancient building or important statue neither violates the principle of unnecessary suffering nor constitutes a *prima facia* violation of the principle of distinction. However, due to broad agreement regarding how important cultural property is to the civilian population, and the intangible effects such as its intrinsic value or the loss of enjoyment by future generations, the international community developed a consensus to place these objects under special protection. Specifically, the Convention for the Protection of Cultural Property acknowledges that "the preservation of the cultural heritage is of great importance for all peoples of the world and that it is important that this heritage should receive international protection . . . ."[133]

Additionally, the support for such a unique LOAC restriction derived from the fact that there was some historical precedent recognizing the importance of cultural property to the civilian population. The Convention for the Protection of Cultural Property notes that it was "[g]uided by the principles concerning the protection of cultural property during armed conflict, as established by the Conventions of The Hague of 1899 and of 1907 and in the Washington Pact of 15 April, 1935."[134]

In the case of submarine cables, such a treaty would require States to recognize that the free flow of data between continents and the preservation of the global economic and social order is more crucial than the military advantage of degrading a belligerent's command and control capability during armed conflict. Mainly, mitigating harm to civilians during all-domain operations requires a new approach to taking feasible precautions that avoid non-kinetic, intangible injury to the civilian population. As shown above, there have been various historical attempts to prohibit the targeting of submarine cables in wartime. Each attempt failed not because

---

[131] Protocols prohibiting or regulating such weapons, as well as non-detectable fragments, mines, booby-traps, incendiary weapons, lasers, and remnants of war, were later adopted.
[132] *See* TALLINN MANUAL, *supra* note 96, at 420.
[133] *See generally* Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, *supra* note 130, S. TREATY DOC. NO. 106-1, at 16, 249 U.N.T.S. at 240.
[134] *Id.* (citations omitted).

of significant differences in principle, but for other reasons specific to the time and place. However, just as the international community went beyond the cardinal principles of LOAC to recognize the necessity to mitigate the "knock-on" effects of targeting cultural property, so too can it create a legal instrument designed to protect submarine cables.

C. State Practice and Customary International Law

Recent scholarship has included a thorough analysis of a customary international law [135] approach to protecting submarine cables in peacetime.[136] The difficulties with developing customary international law for peacetime protection—mainly creating a consensus in today's political environment—are all the more difficult and lead to greater dangers in armed conflict.

Difficult does not mean impossible, however, as it has been done before. The Truman Proclamation is one example of how State practice created customary international law and paved the way for the development of treaty law.[137] In 1945, President Harry Truman declared "the natural resources of the subsoil and sea bed of the continental shelf beneath the high seas but contiguous to the coasts of the United States as appertaining to the United States, subject to its jurisdiction and control."[138] This proclamation, which at the time was a "radical departure" from the law of the sea, eventually led to the 1958 Geneva Conference on the Law of the Sea.[139] It could be argued that the 1958 Geneva Conference, and from there UNCLOS, served as affirmation of unilateral State action that is taken in support of molding customary international law to reflect reality and technological advances.

---

[135] *See* LAW OF WAR MANUAL, *supra* note 6, § 1.8 ("*Customary international law* results from a general and consistent practice of States that is followed by them from a sense of legal obligation (*opinio juris*). Customary international law is an unwritten form of law in the sense that it is not created through a written agreement by States. Customary international law is generally binding on all States, but States that have been persistent objectors to a customary international law rule during its development are not bound by that rule. Assessing whether State practice and *opinio juris* have resulted in a rule of customary international law may be a difficult inquiry." (citations omitted)).

[136] *See, e.g.*, Lieutenant Commander Elizabeth Anne O'Connor, *Underwater Fiber Optic Cables: A Customary International Law Approach to Solving the Gaps in the International Legal Framework for Their Protection*, 66 NAVAL L. REV. 29 (2020).

[137] *Id.* at 43.

[138] Proclamation No. 2667, 10 Fed. Reg. 12303 (Oct. 2, 1945).

[139] O'Connor, *supra* note 136, at 44.

With regard to submarine cables, a proclamation declaring that (1) targeting submarine cables that connect the United States to another State constitutes an armed attack that would justify the use of force in self-defense and (2) targeting submarine cables in armed conflict is a violation of the principles of LOAC would not be a "radical departure" from today's international law. On the contrary, experts behind law of war publications such as the *Oxford, San Remo, Tallinn,* and *Oslo Manuals* already recognize the importance of submarine cables and have declared, with some relatively significant exceptions and caveats, that submarine cables deserve protection. Such a proclamation would be similar to adopting a "no first use" policy[140] declaring that, unlike in all the past conflicts discussed above, commencement of hostilities will not include the targeting of submarine cables. Given "the justifications for protecting underwater fiber optic cables are universal,"[141] this approach may begin to build diplomatic and political consensus toward future treaty efforts to legally prohibit the targeting of submarine cables. At the very least, it may effect customary international law in the practice of naval warfare.

VIII. Conclusion

While the changing character of war requires commanders and their legal advisers to develop an understanding of emerging issues related to all-domain threats, targeting submarine cables is an illustrative example of how it should also drive them to think of old issues in new ways. Since Admiral Dewey's actions in Manila Bay, navies have often legally targeted submarine cables on the basis that they are a valid military objective. However, given that technological advancements have made today's global economic and social order dependent on submarine cables, their destruction would have a significant and harmful impact on the civilian population.

One of the purposes of international law as it relates to the regulation of armed conflict is to enforce the principle that "the civilian population enjoys general protection from the effects of hostilities."[142] Although LOAC prevents the targeting of civilian objects, which most submarine cables inherently are, they are considered military objectives, and thus lawful targets, under the dual-use principle. Additionally, despite the likelihood

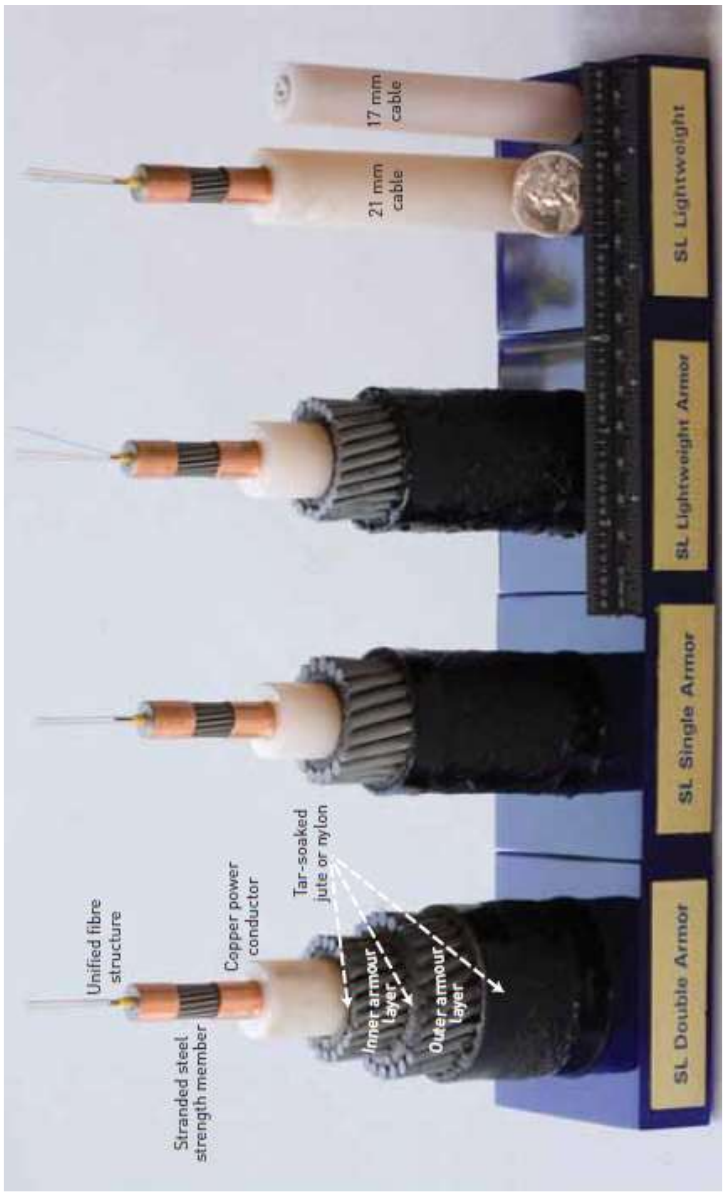
---

[140] AMY F. WOOLF, CONG. RSCH. SERV., IN10553, U.S. NUCLEAR WEAPONS POLICY: CONSIDERING "NO FIRST USE" (2021).
[141] O'Connor, *supra* note 136, at 49.
[142] TALLINN MANUAL, *supra* note 96.

that the destruction of a few submarine cables could have a harmful impact on the civilian population, they remain lawful targets because, under the traditional application of determining what is "excessive," the destruction of the cable itself would not outweigh the military advantage.[143] However, as the character of war has changed and civilian reliance on submarine cables has increased, LOAC must not only reflect the protective status of the tangible cable, but also seek to protect the intangible data it transmits and avoid the devastating "knock-on" effects that would result from its targeting. Therefore, modern warfare requires new approaches to LOAC, such as the development of international law that prohibits the targeting of submarine cables.

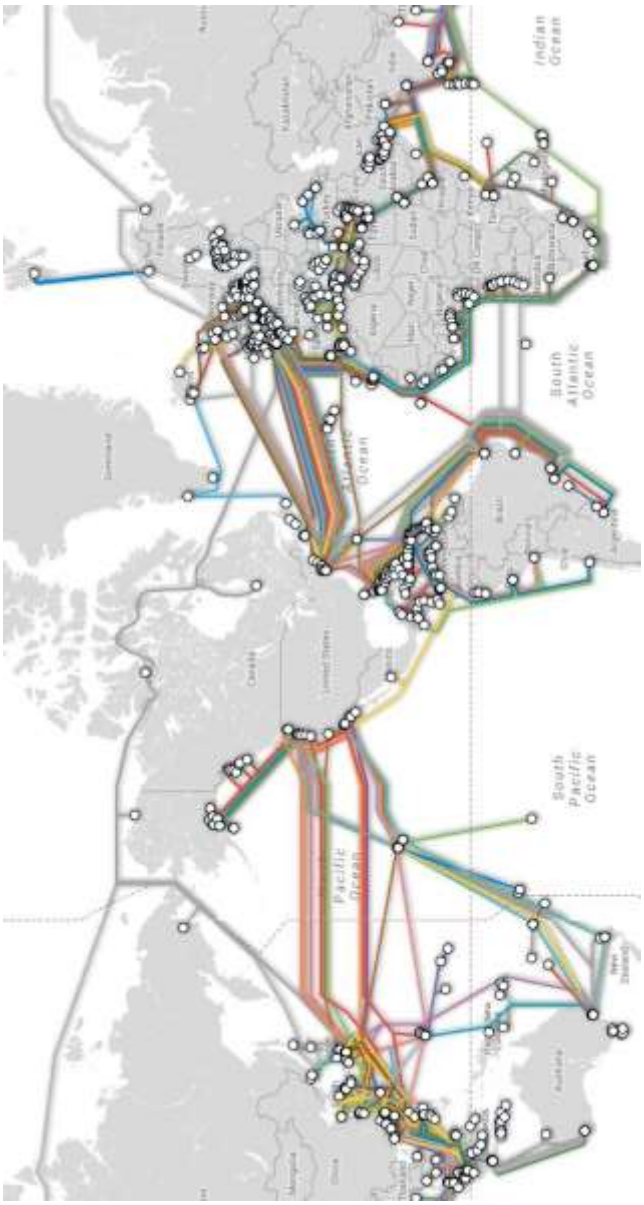
[143] LAW OF WAR MANUAL, *supra* note 6, § 5.12.3.

Appendix A. Photograph of fiber optic submarine cable.[*]



[*] CARTER ET AL., *supra* note 30, at 18.

Appendix B. Map of majority of submarine cable systems.*



* *Cable Data*, INT'L CABLE PROT. COMM., https://www.iscpc.org/information/cable-data (last updated Sept. 29, 2014).

MEDALS "RIDICULOUSLY GIVEN"? THE AUTHORITY TO AWARD, REVOKE, AND REINSTATE MILITARY DECORATIONS IN THREE CASE STUDIES INVOLVING EXECUTIVE CLEMENCY

DWIGHT S. MEARS*

I. Introduction

In November 2019, then-president Donald Trump stirred controversy when he issued pardons to Clint Lorance and Mathew Golsteyn and reversed the demotion of Edward Gallagher—all current or former military Service members accused or convicted of serious crimes during active armed conflict. A number of the former president's actions were without precedent: in Golsteyn's case, a Service member accused of law of armed conflict violations had never before received a pardon prior to trial;[1] in Gallagher's case, a President had never before intervened in a law of armed conflict prosecution before conviction,[2] prevented revocation of Special Forces insignia,[3] or punished a prosecution team by revoking their achievement

* Major (Retired), U.S. Army. M.L.I.S., 2019, San Jose State University, San Jose, California; J.D., 2017, Lewis & Clark Law School, Portland, Oregon; Ph.D. (U.S. History), 2012, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina; M.A. (U.S. History), 2010, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina; B.S. (American Legal System Field of Study), 2001, U.S. Military Academy, West Point, New York. Legal publications include: Dwight S. Mears, *"Neither an Officer nor an Enlisted Man": Contract Surgeons' Eligibility for the Medal of Honor*, 85 J. MIL. HIST. 51 (2021); DWIGHT S. MEARS, THE MEDAL OF HONOR: THE EVOLUTION OF AMERICA'S HIGHEST MILITARY DECORATION (2018); Dwight S. Mears, *Neutral States and the Application of International Law to United States Airmen in World War II. To Intern or Not to Intern?*, 15 J. HIST. INT'L L. 77 (2013); Dwight S. Mears, *Better Off as Prisoners of War. The Differential Standard of Protection for Military Internees in Switzerland During World War II*, 15 J. HIST. INT'L L. 173 (2013). I would like to thank Lieutenant Colonel Dan Maurer, Lieutenant Colonel (Retired) Michael J. Davidson, Eugene Fidell, Colonel (Retired) Erik Winborn, Colonel (Retired) Fred Borch, Major General (Retired) Michael Nardotti, and Major General (Retired) Walter Huffman for their feedback on this article.

[1] *See* Lieutenant Colonel Dan Maurer, *Should There Be a War Crime Pardon Exception?*, LAWFARE (Dec. 3, 2019, 9:31 AM), https://www.lawfareblog.com/should-there-be-war-crime-pardon-exception (documenting that Donald Trump is the first President to pardon Soldiers for offenses that violate the law of armed conflict, either before or after conviction).

[2] Sam LaGrone, *Updated: President Trump Tweets to Stop Gallagher Trident Review Board*, USNI NEWS, https://news.usni.org/2019/11/21/president-trump-tweets-to-stop-gallagher-trident-review-board (Nov. 22, 2019, 6:43 AM).

[3] Meghann Myers & Carl Prine, *Esper Explains Why Navy Secretary Was Fired Over Double-Talk in SEAL Trident Controversy*, MIL. TIMES (Nov. 25, 2019), https://

medals.[4] While the media's coverage of these events was extensive, the focus on the prosecutions largely overshadowed the impact on eligibility for and retention of military decorations.

These distinct case studies provide insight into the potential effects of pardons on retroactive service medal eligibility, the ability to revoke and then restore valor medals, as well as the ability to revoke medals already lawfully awarded and presented. They illustrate that the full scope of authority to deny or revoke achievement or valor medals is unclear in both the governing statute and some regulations and has not been uniformly applied between the services. This ambiguity and inconsistency has resulted in award revocations that could be overturned by administrative boards or in Federal court. To avoid such an outcome, the limits of revocation authority should be further clarified by policy, statute, or both.

II. Military Decorations and Honorable Service

A. First U.S. Military Awards

Military decorations and awards were introduced in the nascent U.S. military during the Revolutionary War, when General George Washington established the Badge of Military Merit on his own authority to "encourage every species of Merit."[5] However, the badge quickly fell into disuse.[6] Military awards proved unpopular in the early Republic, partly due to their association with European aristocracy and the perception that they were undemocratic.[7] It was not until the Civil War that the first lasting military award, the Medal of Honor, was authorized by statute to "furnish a great stimulus to exertion" initially for Service members in the Navy and, later, the Army.[8]

---

www.militarytimes.com/news/your-military/2019/11/25/secdef-explains-why-navy-secretary-was-fired-over-double-talk-in-seal-trident-controversy.

[4] Colby Itkowitz, *Trump Orders Lawyers' Achievement Awards Revoked in Navy SEAL Murder Case*, WASH. POST (July 31, 2019), https://www.washingtonpost.com/politics/trump-orders-lawyers-achievement-awards-revoked-in-navy-seal-murder-case/2019/07/31/11a74d2c-b3cf-11e9-951e-de024209545d_story.html.

[5] DWIGHT S. MEARS, THE MEDAL OF HONOR: THE EVOLUTION OF AMERICA'S HIGHEST MILITARY DECORATION 13 (2018).

[6] *Id.*

[7] *Id.* at 10.

[8] *Id.* at 13–14.

The Medal of Honor was intended as a tool to incentivize desired behavior and improve morale. In the award's infancy, it was the only tangible medal available to reward gallantry, achievement, or service in any branch of the military.[9] Its governing statutes, however, listed little in the way of eligibility criteria and delegated authority to the heads of the military services to award as they saw fit.[10] In the case of the Army, no regulations existed for the medal until 1897, some 35 years after its authorization.[11] This policy vacuum later led to the perception that a great many medals were awarded on dubious merits, which vicariously tainted other recipients by lowering the general prestige of the decoration.[12] This finally spurred the Army to develop exacting criteria to elevate the decoration at the turn of the twentieth century.[13] One of these new requirements was honorable service, which was likely intended as a method of sorting through the relative merit of the many hundreds of retroactive claimants who petitioned the Army for the Medal of Honor.[14]

B. Honorable Service Requirement

Military decorations trace the requirement for honorable service to 1903, when the War Department issued a general order stipulating that "[n]either a medal of honor nor a certificate of merit will be awarded in any case when the service of the person recommended, subsequent to the time when he distinguished himself, has not been honorable."[15] The Medal of Honor was still the only tangible decoration in the Army at this time, which firmly tied the requirement for subsequent honorable service to valor decorations.[16] The same regulatory provision was interpreted to include campaign badges[17] in 1905.[18] In 1918, the provision was added to the Army's appropriations bill that authorized new and existing medals during World War I; the bill provided that "no medal, cross, bar, or other device,

---

[9] *See id.* at 40, 64–68. The Certificate of Merit was converted to a badge in 1905 and other valor decorations were authorized by executive order and statute in 1918. *Id.*
[10] *Id.* at 13.
[11] *Id.* at 21.
[12] *Id.* at 43.
[13] *Id.* at 27.
[14] *Id.* at 36–37.
[15] U.S. Dep't of War, Gen. Order No. 28, para. 199½ (Mar. 12, 1903).
[16] MEARS, *supra* note 5, at 64–68.
[17] Campaign badges were the precursor to campaign medals, and they were awarded for participation in specified geographical theaters during a discrete time period. *Id.* at 40.
[18] U.S. Dep't of War, Circular 17 (Mar. 31, 1905).

hereinbefore authorized, shall be awarded or presented to any individual whose entire service subsequently to the time he distinguished himself shall not have been honorable."[19] The provision applied only to decorations authorized in that legislation but was subsequently interpreted to apply to all military decorations in the Army.[20] The same provision applied equally to the Air Force, since at the creation of the Air Force as a separate branch, it inherited much of the Army's statutory authority for military awards.[21]

The Navy received the "subsequent honorable service" provision in a 1919 bill that contained military award provisions substantially borrowed from the Army's companion bill enacted the prior year.[22] The Navy's bill specified "[t]hat no medal or cross or no bar or other emblem or insignia shall be awarded or presented to any individual or to the representative of any individual whose entire service subsequent to the time he distinguished himself shall not have been honorable."[23] This provision was more expansive than the Army's, as it already covered all existing and future Navy decorations.

The requirement for honorable service was eventually expanded in regulations for all branches of the military, soon growing well beyond mere "subsequent" service. Today, various regulations add to the statutory authority and effectively require honorable service before, during, and after qualification for all military decorations. Regulations also sanction retroactive revocation of medals already awarded and presented, which also has historically been tethered to honorable service.

---

[19] Act of July 9, 1918, Pub. L. No. 65-193, 40 Stat. 845, 872.
[20] *Id.*; U.S. DEP'T OF WAR, ARMY REGULATIONS para. 188 (Nov. 15, 1913) (C80, Sept. 17, 1918) (specifying that "[n]o medal of honor, distinguished-service cross, distinguished-service medal, or bar, or ribbon shall be awarded or presented to any individual whose entire service subsequent to the time he distinguished himself shall not have been honorable").
[21] MEARS, *supra* note 5, at 116; U.S. DEP'T OF ARMY & U.S. DEP'T OF AIR FORCE, REG. 1-11-53, TRANSFER OF FUNCTIONS PERTAINING TO DECORATIONS AND AWARDS para. 2*b* (20 Dec. 1948).
[22] MEARS, *supra* note 5, at 74.
[23] Act of Feb. 4, 1919, Pub. L. No. 65-253, 40 Stat. 1056, 1057.

III. Clint Lorance and Eligibility for a Campaign Medal

A. Background

Clint Lorance, then a U.S. Army first lieutenant and platoon leader deployed to Afghanistan, ordered one of his Soldiers to open fire on several unarmed Afghan motorcyclists in July 2012.[24] He claimed that the rules of engagement had been modified to allow firing on any motorcycle, which he reportedly knew was untrue.[25] Two unarmed Afghans were killed in the resultant shooting, which amounted to gunning down men who posed no apparent threat at the time.[26] Lorance subsequently falsified a report about the incident and claimed that the victims could not be assessed because the bodies had been removed by local villagers.[27] He was turned in by one of his own Soldiers,[28] leading to his conviction by court-martial for murder and other charges and an approved sentence of nineteen years' confinement, dismissal from the service, and forfeiture of all pay and allowances.[29]

Lorance also presumably had his Afghanistan Campaign Medal suspended and administratively revoked[30] as a "collateral consequence"[31] of court-martial. That medal is normally awarded automatically upon tour completion, based solely on having served within the "land area of the country of Afghanistan and all airspaces above the land" for a specified period of time.[32] Then-president Trump later pardoned Lorance under the dubious rationale that the motorcyclists had approached "with unusual speed," and that the lieutenant was merely "prioritizing the lives of

---

[24] United States v. Lorance, No. ARMY 20130679, 2017 WL 2819756, at *2 (A. Ct. Crim. App. June 27, 2017).
[25] Dave Philipps, *Cause Célèbre, Scorned by Troops*, N.Y. TIMES (Feb. 24, 2015), https://www.nytimes.com/2015/02/25/us/jailed-ex-army-officer-has-support-but-not-from-his-platoon.html.
[26] *Lorance*, 2017 WL 2819756, at *2.
[27] *Id.* at *3.
[28] *Id.*
[29] *Id.* at *1.
[30] U.S. DEP'T OF ARMY, REG. 600-8-22, MILITARY AWARDS para. 1-30*b* (5 Mar. 2019) [hereinafter AR 600-8-22].
[31] "A collateral consequence is '"[a] penalty for committing a crime, in addition to the penalties included in the criminal sentence."'" United States v. Talkington, 73 M.J. 212, 215 (C.A.A.F. 2014) (alteration in original) (quoting United States v. Miller, 63 M.J. 452, 457 (C.A.A.F. 2006)).
[32] AR 600-8-22, *supra* note 30, para. 2-17*b*–*c*.

American troops" by ordering the engagement.[33] Whether justified or not, Lorance's pardon raises interesting questions about whether clemency erases a Service member's misconduct and makes them eligible for military decorations that are predicated on honorable service. Lorance's case study demonstrates that a pardon does not in fact erase underlying misconduct, and therefore does not alter award eligibility.

B. Army Service Medals and Honorable Service

Campaign medals like the one Lorance earned and ostensibly lost are a type of service medal based on a period of qualifying service rather than an achievement or gallant action, and they are awarded for having served in a specified geographical theater during an authorized time period.[34] As discussed above, the Army's "subsequent honorable service" provision was interpreted to include the precursor to campaign medals in 1905.[35] The Army expanded this requirement in 1922, stipulating that "[s]ervice medals and clasps may be earned by honorable service only," and that "[s]ervice in an enlistment which was terminated otherwise than honorably is not considered honorable service, within the meaning of the term as here used."[36] Thus, regulations required both the qualifying service and the service afterward to be honorable. The Army's current regulation states that "the military service of the Servicemember on which qualification for award of [campaign, expeditionary, and service] medals is based must have been honorable."[37] With the exception of only one service medal,[38] this authority is regulatory. Most service medals do not trace requirements for honorable service during qualifying periods to statutory authority, since the awards are not authorized by statute in the first place. Service following medal qualification, however, is still covered by the statutory provision on subsequent honorable service.[39]

---

[33] *Statement from the Press Secretary*, WHITE HOUSE (Nov. 15, 2019), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-97.
[34] U.S. Dep't of War, Circular 17 (Mar. 31, 1905).
[35] *Id.*
[36] U.S. DEP'T OF WAR, REG. 600-65, AWARD AND SUPPLY OF SERVICE MEDALS para. 4*a* (Jan. 30, 1922) (C2, Apr. 30, 1925).
[37] AR 600-8-22, *supra* note 30, para. 2-9*d*.
[38] 10 U.S.C. § 1128(f) (listing honorable service as a prerequisite for the prisoner-of-war medal).
[39] *Id.* § 1136.

Honorable service throughout the entire qualifying period is a fundamental prerequisite for service medals; thus, any less-than-honorable service is a basis for award denial. While there is no precise threshold for what constitutes "honorable" service,[40] it often corresponds to conduct that merits retention in the service.[41] According to Army regulations, a determination of honorable service for the purpose of medal qualification "will be based on such honest and faithful service according to the standards of conduct, courage, and duty required by law and customs of the service of a Servicemember of the grade to whom the standard is applied."[42]

The Army's regulatory requirement for honorable service ostensibly prevented Lorance from receiving an Afghanistan Campaign Medal based on the misconduct underlying his court-martial conviction and the administrative determination that his qualifying service in Afghanistan was not honorable.[43] His subsequent pardon, however, could potentially change this outcome depending on its effect on his underlying service. Normally, Lorance would qualify for the medal based solely on time in theater; regulations require thirty consecutive days at a minimum, and he had several months.[44] Participating in an armed engagement is another method to qualify for the decoration without respect to time in theater.[45] Thus, somewhat ironically, the same unauthorized engagement that branded Lorance a murderer could be used to establish his eligibility, but only if his pardon truly has the effect of erasing his misconduct.

C. Impact of Pardons on Underlying Offenses

Several precedents inform the question of whether pardons erase the underlying offense. In the 1866 case of *Ex parte Garland*, the Supreme Court struck down a law that prevented attorneys from practicing before certain courts unless they could swear they had "never voluntarily borne arms against the United States" or "exercised the functions of any office

---

[40] *But see* U.S. DEP'T OF ARMY, REG. 635-200, ACTIVE DUTY ENLISTED ADMINISTRATIVE SEPARATIONS para. 3-7*a* (19 Dec. 2016) (defining "honorable" service at separation).
[41] U.S. DEP'T OF DEF., INSTR. 1348.33, DOD MILITARY DECORATIONS AND AWARDS PROGRAM sec. 8 (Dec. 21, 2016) (C5, Apr. 9, 2021).
[42] AR 600-8-22, *supra* note 30, para. 1-17*a*.
[43] *Id.* paras. 1-17*a*(1), 1-30*b*.
[44] *Id.* para. 2-17*c*; Michelle Tan, *Hero or Murderer? Soldiers Divided in 1LT Lorance Case*, ARMY TIMES (Jan. 12, 2015), https://www.armytimes.com/news/your-army/2015/01/12/hero-or-murderer-soldiers-divided-in-1lt-lorance-case.
[45] AR 600-8-22, *supra* note 30, para. 2-17*c*.

. . . in hostility to the United States."[46] Garland, a former member of the Confederate Congress, had received a full pardon from President Lincoln but was still barred from practicing on account of his inability to take this oath.[47] The Court ruled that the law in question was "in direct opposition to the constitutional effect of the pardon," explaining that perpetual disqualification amounted to Congress "punish[ing] the petitioner for the same offence" by denying him a property right.[48] In dicta, the Court expressed that "when the pardon is full, it releases the punishment and blots out of existence the guilt, so that in the eye of the law the offender is as innocent as if he had never committed the offence."[49] This portion of the opinion was never exercised literally, as both courts and executive officials repeatedly determined that a pardon did not actually expunge the record of an offense.

In 1898, the Attorney General considered how a pardon interacted with a law that required prior honorable service as a prerequisite for reenlistment.[50] Private Daniel T. Thompson had been convicted of desertion from the 7th Infantry and was dishonorably discharged.[51] After he received a full pardon from the President, he applied for reenlistment. The applicable statute stated that "no soldier shall be again enlisted in the Army whose service during his last preceding term of enlistment has not been honest and faithful."[52] The Attorney General reasoned that the bar on enlistment was lawful because it did not necessarily flow from a conviction; after all, "[t]here are many acts of a soldier which may be regarded under the strict rules of the requirements of the military service as unfaithful or dishonest, but of which a military court-martial would not take cognizance."[53] Many potential actions that would bar reenlistment were not impacted by pardons since they "do not reach that grade of offense which would authorize the exercise of executive clemency."[54] In the Attorney General's view, "Congress has the right to prescribe qualifications and conditions for

[46] *Ex parte* Garland, 71 U.S. (4 Wall.) 333, 376 (1866).
[47] Michele E. Boardman, Whether a Presidential Pardon Expunges Judicial and Executive Branch Records of a Crime, 30 Op. O.L.C. 104, 108 (2006).
[48] *Garland*, 71 U.S. at 340, 347.
[49] *Id.* at 380.
[50] Army—Enlistment—Pardon, 22 Op. Att'y Gen. 36 (1898).
[51] *Id.* at 37.
[52] Act to Regulate Enlistments in the Army of the United States, 28 Stat. 215, 216 (1894).
[53] *Army—Enlistment—Pardon*, 22 Op. Att'y Gen. at 39.
[54] *Id.*

enlisted men."[55] He ruled that a pardon merely "relieves [a criminal] of the disabilities legally attaching to his conviction," but "does not destroy an existing fact, viz, that his service was not honest and faithful."[56]

Subsequent Supreme Court decisions affirmed that a pardon does not in fact "blot out" guilt entirely. In *Carlesi v. New York*, the Court expressed that the judiciary could use prior pardoned offenses as circumstances of aggravation for another crime.[57] The Court reasoned that the practice was not *ex post facto*, as it merely punished "future crimes" and thus was not "in any degree a punishment for [a] prior crime."[58] In *Burdick v. United States*, the Court held that a pardon could be refused due to the "guilt implied in the acceptance"[59] and that acceptance of a pardon stands as "a confession of guilt."[60] Of course, both of these cases are clearly incompatible with the notion that a pardon entirely erases the record of an offense.

In 1918, the Attorney General opined on the ability of a pardoned former Navy officer to reenter the active Navy or the Fleet Naval Reserve in spite of his dismissal by court-martial.[61] Per statute, honorable discharge was a requirement for both appointments.[62] According to the Attorney General, the key question was whether the statutory restriction was "punishment for an offense" or "a qualification for appointees to office in the Navy."[63] He ultimately determined that the statute did not "impose a penalty as such on individual offenders," and that its "incidental disabilities . . . are not removed by a pardon."[64] The Attorney General explained that a pardon "abates whatever punishment flows from the commission of the pardoned offense," but could not "eradicate the *factum* which is made a criterion of fitness."[65] However, the outcome changed in the case of a different statute that perpetually stripped military deserters of the ability to hold office, as well as citizenship rights, even after issuance of a pardon. Here, in the Attorney General's view, the statute imposed disabilities "not

---

[55] *Id.*
[56] *Id.*
[57] Carlesi v. New York, 233 U.S. 51, 59 (1914).
[58] *Id.* at 57, 58.
[59] Burdick v. United States, 236 U.S. 79, 91 (1915).
[60] *Id*. at 94.
[61] Naval Service—Desertion—Pardon, 31 Op. Att'y Gen. 225 (1918).
[62] *Id.* at 226.
[63] *Id.*
[64] *Id.* at 230.
[65] *Id.* at 227.

merely incidental to rules prescribing the qualifications for service in the Navy," but rather as "penalties for the punishment of offenses."[66] Therefore, the distinction between the two laws was that one was a legitimate congressional regulation of military fitness criteria, while the other was a clear punishment that imposed impermissible restrictions on civil rights after a pardon.

In 1927, The Judge Advocate General of the Army ruled that a pardoned Soldier remained ineligible for a campaign medal under a regulation implementing the "subsequent honorable service" provision.[67] Though the Soldier in question had served honorably during service in the Philippines, he was convicted of desertion during a subsequent enlistment and dishonorably discharged.[68] After receiving a full and unconditional pardon from the President, the Soldier applied for a Philippine Campaign Medal under the theory that his service during that enlistment was qualifying because the pardon removed the subsequent misconduct.[69] Regulations allowed the medal's retroactive approval so long as the Soldier had "subsequently to the last nonhonorable service been in an honorable status in the Army."[70] Since the Soldier had not served honorably after the less-than-honorable service resulting in conviction, The Judge Advocate General ruled that the pardon did not relieve him of the taint of misconduct.[71] This demonstrates that the Army understood a pardon's function as removing punishment, not erasing prior misconduct as if it had never occurred. In context, the withholding of a medal was not a penalty for a crime. Rather, it was mere regulation of eligibility criteria ostensibly intended to protect the inherent value of the decoration to other past and future recipients.

The Judge Advocate General of the Army established another precedent in 1947 by ruling that an Army Air Force colonel's Legion of Merit could be disapproved for less than a court-martial conviction.[72] Specifically, the colonel was disciplined after his period of qualifying service for

---

[66] *Id.* at 232.
[67] U.S. DEP'T OF WAR, DIGEST OF OPINIONS OF THE JUDGE ADVOCATE GENERAL OF THE ARMY: 1912–1930 sec. 389 (1932).
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] U.S. DEP'T OF ARMY, BULLETIN OF THE JUDGE ADVOCATE GENERAL OF THE ARMY, JANUARY–FEBRUARY 1947, at 46 (1947).

"'reprehensible . . . gross misconduct' of such a nature as to make him an object of contempt and a discredit to the service."[73] The Judge Advocate General opined that this characterization precluded a determination that the colonel's entire period of service was honorable under the governing regulation, which required that "no decoration shall be awarded or presented to any individual whose entire service subsequent to the time he distinguished himself shall not have been honorable."[74] Thus, actions not reaching a criminal threshold could nevertheless be determined as a departure from the honorable service required by the statute. This demonstrates that the effect of the "subsequent honorable service" provision was not interpreted as a penalty for a crime, but as a screening mechanism for underlying conduct that was disreputable to the individual and their branch of military service.

D. Impact of Pardons on Expungement

Federal appellate cases have also ruled that pardons do not result in automatic expungement of records, though the issue has not yet reached the Supreme Court. In the Third Circuit case of *United States v. Noonan*, a draft evader was convicted of violating the Military Selective Service Act and subsequently pardoned.[75] The pardonee petitioned to have his conviction expunged due its impact on his employment prospects, claiming that the pardon should automatically result in both the erasure of his indictment "as if it had never occurred" and the impoundment of all records pertaining to his arrest and conviction.[76] On appeal, the Third Circuit reasoned that the President's authority to expunge criminal records "must stem either from an act of Congress or from the Constitution itself" and that no such authority existed.[77] The court deemed the pardon power as "an executive prerogative of mercy, not of judicial record-keeping."[78] In reversing the expungement request, the court reflected that "to tamper with judicial records" would "[fly] in the face of the separation of powers doctrine."[79] Similar rulings on

---

[73] *Id.*
[74] *Id.* (quoting U.S. DEP'T OF WAR, REG. 600-45, DECORATIONS para. 19 (22 Sept. 1943)).
[75] United States v. Noonan, 906 F.2d 952, 953–54 (3d Cir. 1990).
[76] *Id.* at 954.
[77] *Id.* at 955 (citing Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585 (1952)).
[78] *Id.*
[79] *Id.* at 956.

expungement were subsequently issued by the D.C.,[80] Seventh,[81] and Ninth Circuits.[82]

The Department of Justice's Office of Legal Counsel adopted the *Noonan* holding in a 2006 opinion on the impact of a presidential pardon authored for the United States Pardon Attorney.[83] The Office of Legal Counsel concluded that a pardon "does not operate to erase automatically the records relating to the pardoned offense," and that "[t]he relevant judicial and executive records preserve an important set of historical facts concerning the individual's criminal history."[84] However, the Office of Legal Counsel also opined that a President might order the expungement of records separate from a pardon, which might be successful unless prevented by "any statutory constraints on executive record-keeping."[85] The Department of Justice's position on the effects of pardons has not changed in this respect. Its website on pardon information states that, "[w]hile a presidential pardon will restore various rights lost as a result of the pardoned offense and should lessen to some extent the stigma arising from a conviction, it will not erase or expunge the record of [one's] conviction."[86] Further, the website warns pardon applicants that a "[p]ardon of a military offense will not change the character of a military discharge."[87]

E. Impact of Pardon on Lorance

Applied to Lorance's case, the denial of a campaign medal due to less-than-honorable service is squarely in accord with law, policy, and precedent. The mere issuance of a pardon does not erase the fact of his less-than-honorable service, and therefore the misconduct underlying a conviction may be used to deny military awards due to the failure to satisfy the honorable service requirement. Interpreted most favorably to Lorance, the denial of an award could subjectively be seen as a penalty or punishment, considering that it was a collateral consequence of his court-martial. On

---

[80] *In re* North, 62 F.3d 1434, 1437 (D.C. Cir. 1994).
[81] Hirschberg v. Commodity Futures Trading Comm'n, 414 F.3d 679 (7th Cir. 2005).
[82] United States v. Bays, 589 F.3d 1035 (9th Cir. 2009).
[83] Whether a Presidential Pardon Expunges Judicial and Executive Branch Records of a Crime, 30 Op. O.L.C. 104 (2006).
[84] *Id.* at 110.
[85] *Id.*
[86] *Pardon Information and Instructions*, U.S. DEP'T OF JUST., https://www.justice.gov/pardon/pardon-information-and-instructions (Nov. 23, 2018).
[87] *Id.*

the other hand, as with the case of Private Daniel T. Thompson, the bar of less-than-honorable service was not exclusively applicable to misconduct leading to court-martial convictions. Honorable service prerequisites have been interpreted to preclude awards for a broad spectrum of misconduct that may not result in trial by court-martial, including any service that is not "honest and faithful."[88] Further, military regulations do not refer to the effects of the "honorable service" provision as a penalty or punishment, and there is no evidence that the provision was crafted for this purpose. Indeed, when the first "honorable service" provision for the Medal of Honor appeared in Army regulations, it contained no clear explanation of underlying intent.[89] In context, during this period the Army received petitions from many separated Soldiers who sought retroactive awards.[90] Thus, the most likely explanation is that the Army sought to restrict medal eligibility based on the category of service, both as a matter of efficiency and to elevate the prestige of the decoration. This would make the provision incidental to regulation of the award itself and not a penalty for court-martial conviction.

Finally, Lorance's case is similar to the 1927 ruling of The Judge Advocate General of the Army, in which a Soldier had been convicted of an offense by court-martial and received an unconditional pardon. That Soldier was barred from receipt of a campaign medal based on the fact of his misconduct after his qualifying service—the act of desertion, which ran afoul of the requirement for subsequent honorable service. Similarly, Lorance's pardon does not erase his conviction or the fact that his underlying service—which included murder—was less-than-honorable. The primary difference is that Lorance's misconduct occurred during his qualifying period of service, and the deserter's followed. However, they were both instances where less-than-honorable service correctly precluded the award of a campaign medal, even after issuance of an unconditional pardon.

IV. Mathew Golsteyn and Revocation of a Valor Award

A. Background

In February 2010, Mathew Golsteyn, then a captain in the U.S. Army, allegedly detained a bomb-maker suspected of attacking U.S. forces in his

---

[88] AR 600-8-22, *supra* note 30, para. 1-17*a*.
[89] U.S. Dep't of War, Gen. Order No. 28, para. 199½ (Mar. 12, 1903).
[90] MEARS, *supra* note 5, at 40–41.

area of operations, Forward Operating Base McQueary, Afghanistan. According to a U.S. Army Criminal Investigation Command report, Golsteyn conspired with other members of his Special Forces team to surreptitiously detain and murder the bomb-maker, then "buried him in a shallow grave, and later returned to burn the remains."[91] The Army's criminal investigators were unaware of the incident until Golsteyn sat for a polygraph test in September 2011 while interviewing for a position at the Central Intelligence Agency. Golsteyn allegedly admitted to the polygraph examiner that he had detained, killed, and buried the unarmed bomb-maker.[92] This led to a criminal investigation, but the Army initially declined to charge Golsteyn for lack of corroborating evidence.[93]

Instead of immediately facing charges under the Uniform Code of Military Justice, Golsteyn was administratively reprimanded by a general officer, who cited "a serious departure from the high standards of integrity and professionalism expected of a Commissioned officer of th[at] command," specifically Golsteyn's admission to a "Law of Armed Conflict violation."[94] In addition, Golsteyn's valor decoration—a Silver Star earned for gallantry in action during the same tour—was administratively revoked after presentation on the basis of service that was "less than honorable."[95] The Silver Star had been recommended after a firefight with enemy snipers on 20 February 2010, when Golsteyn "repeatedly exposed himself to direct and accurate enemy fire during a four-hour engagement."[96] Golsteyn was praised for his "calm demeanor, decisive actions and fearlessness in the face of the enemy," specifically for running "approximately 150 meters under

---

[91] CRIM. INVESTIGATION COMMAND, U.S. DEP'T OF ARMY, 0906-2011-CID023-43647-5H1A, CID REPORT OF INVESTIGATION - FINAL/SSI - 0906-2011-CID023-43647-5H1A/5X5/5X4/5X1/5Y2B0/9J, at 26 (2013) [hereinafter GOLSTEYN REPORT OF INVESTIGATION].

[92] *Decorated US Soldier 'Admitted Murder in CIA Job Interview,'* BBC NEWS (Dec. 14, 2018), https://www.bbc.com/news/world-us-canada-46573452; Mathew Golsteyn, No. AR20200000309, Army Bd. for Corr. of Mil. Records 4 (June 26, 2020).

[93] Ryan Devereaux & Jeremy Scahill, *Documents: Green Beret Who Sought Job at CIA Confessed to Murder*, INTERCEPT (May 6, 2015, 7:26 PM), https://theintercept.com/2015/05/06/golsteyn.

[94] *U.S. Army Documents on Major Mathew Golsteyn*, INTERCEPT (May 6, 2015, 7:25 PM), https://theintercept.com/document/2015/05/06/u-s-army-documents-major-mathew-golsteyn.

[95] *Id.*

[96] *Matthew* [sic] *L. Golsteyn*, HALL OF VALOR PROJECT, https://valor.militarytimes.com/hero/52976 (last visited Aug. 27, 2021).

heavy machine gun and sniper fire" to retrieve a Carl Gustaf recoilless rifle and then using the weapon to decisive effect.[97]

Golsteyn's Silver Star was revoked on the basis of misconduct that the Army believed "occurred prior to" and was "distinctly separate" from his heroic actions,[98] but the exact timing of the alleged murder remains obscure due to a lack of witness testimony.[99] Thus, it is unclear whether the misconduct fell within the textual parameters of the "subsequent honorable service" provision, as it apparently occurred days before his service qualifying him for the Silver Star.[100] However, as discussed below, the "honorable service" provision is not the only authority to revoke military decorations. Golsteyn's Silver Star had previously been approved for upgrade to a higher medal, the Distinguished Service Cross, as part of a review meant to remedy a lack of valor decorations.[101] The upgraded award was also suspended and revoked prior to presentation.[102] Golsteyn's Special Forces tab was similarly revoked by administrative action.[103]

In 2015, an administrative board of inquiry determined that the Army had not proven by a preponderance of the evidence that Golsteyn had committed a law of armed conflict violation, but that sufficient proof existed of conduct unbecoming an officer.[104] The board substantiated an allegation of Golsteyn's "misconduct, moral, or professional dereliction," not only because of the murder, but also because he "took steps to cover it up" and "failed to report all the facts officially and for the record over an extended period of time."[105] Based on this finding, the board recommended that

---

[97] *Id.*
[98] *U.S. Army Documents on Major Mathew Golsteyn*, *supra* note 94; GOLSTEYN REPORT OF INVESTIGATION, *supra* note 91, at 110.
[99] GOLSTEYN REPORT OF INVESTIGATION, *supra* note 91.
[100] *Cf. id.* at 60, 106 (discussing approximate periods of investigation).
[101] *U.S. Army Documents on Major Mathew Golsteyn*, *supra* note 94; MEARS, *supra* note 5, at 132.
[102] *U.S. Army Documents on Major Mathew Golsteyn*, *supra* note 94.
[103] Dave Philipps, *Pardoned Soldier Is Denied Bid to Rejoin Green Berets*, N.Y. TIMES, Jan. 10, 2020, at A21.
[104] Dan Lamothe, *Matt Golsteyn Planned to Join the CIA and Go to Iraq. Now He Faces a Murder Charge.*, WASH. POST (Feb. 9, 2019), https://www.washingtonpost.com/world/national-security/they-do-not-obey-their-own-rules-soldier-facing-murder-case-says-he-must-defend-himself-against-the-army/2019/02/09/a4cdb5b2-2baf-11e9-97b3-ae59fbae7960_story.html.
[105] Mathew Golsteyn, No. AR20200000309, Army Bd. for Corr. of Mil. Records 8 (June 26, 2020).

Golsteyn be separated from the Army with a characterization of service as general (under honorable conditions).[106]

Golsteyn subsequently made an admission to killing the bomb-maker during an interview on Fox News, spurring the Army to reopen its investigation and formally charge him with murder in 2018.[107] In an ironic twist, this interview occurred around the same time the Army's lead criminal investigator in Golsteyn's case was accused of stolen valor relating to his own military decorations—specifically wearing badges and a Purple Heart that he did not earn.[108] In 2019, former president Trump made the unprecedented decision to pardon Golsteyn prior to his trial, explaining that the Soldier's victim had "continue[d] to threaten American troops and their Afghan partners," and that a pardon was "in the interests of justice" due to the protracted nature of the prosecution.[109]

Following his pardon, Golsteyn's attorney announced that he was requesting "reinstatement of everything that was taken from him," including his valor decoration and Special Forces tab.[110] The attorney claimed that the effect of the pardon was to "put [Golsteyn] back in the position he was prior to the allegations,"[111] so that he was "allowed everything, just as if this never happened."[112] According to the attorney, former president Trump had directed that Golsteyn's record be "expunged,"[113] and that the Army's failure to complete this action was a "complete contravention" of

---

[106] Kyle Jahner, *Board: Ex-Green Beret Mathew Golsteyn Should Receive General Discharge*, ARMY TIMES (June 29, 2015), https://www.armytimes.com/news/your-army/2015/06/29/board-ex-green-beret-mathew-golsteyn-should-receive-general-discharge.
[107] Philipps, *supra* note 103.
[108] *See* Todd South, *Lead Investigator in Green Beret Murder Case Pleads Guilty to Stolen Valor Charges*, ARMY TIMES (May 7, 2019), https://www.armytimes.com/news/your-army/2019/05/07/lead-investigator-in-green-beret-murder-case-pleads-guilty-to-stolen-valor-charges (documenting that the investigator pleaded guilty to three specifications of Article 134, UCMJ, and was sentenced to a three-grade reduction).
[109] *Statement from the Press Secretary*, *supra* note 33.
[110] Louis Casiano, *Pardoned Green Beret Matt Golsteyn Seeks Military Awards, Decorations*, FOX NEWS (Nov. 19, 2019), https://www.foxnews.com/us/pardoned-green-beret-matt-golsteyn-seeks-military-awards-decorations.
[111] *Id.*
[112] Philipps, *supra* note 103.
[113] *Id.*

the President's wishes.[114] Nevertheless, the Army refused to reauthorize Golsteyn's Special Forces tab, and his request to reinstate his valor decoration was routed to an administrative board known as the Army Board for Correction of Military Records (ABCMR).[115] While the ABCMR denied all of Golsteyn's requests,[116] the case still raises questions about the ability of a military service or a President to revoke or reinstate a different type of military award than discussed in the Lorance case study—a valor decoration—as well as the impact of an unconditional pardon on the same decoration. Golsteyn's case demonstrates that revocation, while often not linked to statutory authority, is presumptively lawful and is not directly affected by a pardon. On the other hand, the authority for revocation is an obscure patchwork of both statute and regulation that would greatly benefit from clarification.

As in Lorance's case, Golsteyn's eligibility for a military decoration was predicated on the same military regulations and statute requiring honorable service.[117] However, the two cases are different in several respects. Golsteyn claimed the pardon should expunge all records relating to his misconduct, which is a step further than merely arguing that a pardon blots out guilt in the eyes of the law. Golsteyn and Lorance also were facing revocation of different types of medals: Golsteyn's was a valor decoration based on a discrete qualifying action occurring on a single day, while Lorance's was a campaign medal that was predicated on honorable service throughout a qualifying period of time and location. Another difference was the fact that Golsteyn's misconduct apparently preceded his qualifying action, although the precise date of the alleged murder remains elusive. Also unlike Lorance, Golsteyn never was convicted at court-martial, although both medals were apparently revoked by administrative action on the basis of underlying misconduct. Further, at the point of revocation, Golsteyn's

---

[114] Vincent Barone, *Army Denies Special Forces Titles to Soldier Pardoned by Trump*, N.Y. POST (Jan. 9, 2020, 10:20 PM), https://nypost.com/2020/01/09/army-denies-special-forces-title-to-soldier-pardoned-by-trump.

[115] Bryan Bender, *General Denies Request for Pardoned Special Forces Soldier to Regain Elite Patch*, POLITICO (Jan. 9, 2020, 8:37 PM), https://www.politico.com/news/2020/01/09/golsteyn-trump-pardon-special-forces-097053.

[116] Mathew Golsteyn, No. AR20200000309, Army Bd. for Corr. of Mil. Records 11–14 (June 26, 2020).

[117] *See* discussion *supra* Section III.B.

Silver Star had already been awarded and presented, which arguably changes the legal implications because of the vesting of property interests.

B. Army Medal Revocation in the Early Twentieth Century

The intent behind requirements for honorable service[118] is somewhat murkier when used to justify revocation of a medal for valor after it was awarded and presented. At the inception of the "honorable service" provision, in the early twentieth century, medals were seen as property with mostly intrinsic value. Thus, in 1904, the Judge Advocate General of the Army[119] ruled that

> [w]hen a medal is conferred there is included in the grant a conveyance of ownership of the medal, regarded as a chattel, which becomes the property of the grantee, and is subject to such disposition as he may see fit to make it as a part of his personal estate.[120]

Also in 1904, the Judge Advocate General of the Army ruled on a proposal by President Theodore Roosevelt to revoke hundreds of Civil War era Medals of Honor previously awarded under dubious circumstances. The Judge Advocate General opined that revocation would be unlawful due to an administrative *res judicata* doctrine under which "an act or decision of the President cannot be reviewed or reversed by a successor" except under specific exceptions, such as "fraud, mistake in matters of fact arising from errors in calculation, or newly discovered material evidence."[121]

Failure to revoke the contested medals in 1904 eventually led to legislation enacted in 1916 which authorized a one-time review and revocation of Army Medals of Honor if certain *ex post facto* criteria were satisfied.[122] The resulting review revoked 911 awards under this

---

[118] *Id.*

[119] While the senior uniformed attorney in the U.S. Army is currently referred to as "The Judge Advocate General," that position was "the Judge Advocate General" prior to 31 January 1924. THE ARMY LAWYER: A HISTORY OF THE JUDGE ADVOCATE GENERAL'S CORPS, 1775–1975, at 139 (1975).

[120] OFF. OF THE JUDGE ADVOC. GEN., U.S. DEP'T OF WAR, DIGEST OF OPINIONS OF THE JUDGE ADVOCATES GENERAL OF THE ARMY: 1912, at 665 (1912).

[121] Memorandum from the Judge Advoc. Gen. of the Army to Sec'y of War (Sept. 20, 1904).

[122] MEARS, *supra* note 5, at 52.

authorization—all without so much as a hearing afforded to the impacted recipients.[123] One of the affected recipients, Lieutenant Colonel (Retired) Asa Gardiner, a former judge advocate and professor of law at the U.S. Military Academy at West Point, complained that "the possession of a medal is a property right and cannot be lawfully taken away . . . without a judicial hearing and an opportunity to be heard in [my] own behalf."[124] As Gardiner correctly noted, revocation should have raised due process concerns due to the substantial property interest enjoyed by medal recipients, but resolving this issue fell to later generations.[125] The mass revocation also set at least an informal precedent that Medals of Honor could only be revoked with congressional authorization, though this was never articulated in policy. To date, no further legislation to expressly revoke personal military decorations has been enacted and no other Medals of Honor have been revoked.

Early Army regulations never expressly referenced the ability to revoke a decoration and, instead, appeared to contemplate only the denial of a medal prospectively—that is, prior to its award and presentation. Thus, when the Army's 1905 circular expanded the "honorable service" provision to campaign badges, the Secretary of War directed that "the badge may be withheld" rather than revoked.[126] Similarly, The Judge Advocate General of the Army's early precedents did not reference revocation, but merely the denial of awards not yet presented. One prominent example occurred in 1924, when The Judge Advocate General ruled that a valor decoration could not be retroactively awarded to First Lieutenant Arthur Cody, an officer who had been convicted at court-martial for drunkenness on duty.[127] Cody had been commended for gallantry in action in the Philippines in 1913, and became retroactively eligible for the Distinguished Service Cross after the award was authorized in 1918.[128] No such precedents were published

---

[123] *Id.* at 55–61.
[124] *Id.* at 60.
[125] *Id.* at 51–52 (explaining that the same session of Congress also authorized a pension for Medal of Honor recipients).
[126] U.S. Dep't of War, Circular 17 (Mar. 31, 1905).
[127] U.S. DEP'T OF WAR, *supra* note 67, sec. 377; Headquarters, U.S. Dep't of War, Gen. Order No. 116 (Aug. 29, 1917).
[128] *Hero of Many Battles Dies at Post After Remarkable Career*, WKLY. J.-MINER, June 7, 1922, at 1.

for revocation of awards that had already been awarded and presented to recipients, suggesting that the Army was not revoking medals at this time.

C. Evolution of Army Regulations Governing Revocation

Army regulation authorized revocation for a limited purpose unrelated to misconduct starting in 1956: to rescind an "interim award" made "by appropriate authority *pending* final action on a recommendation for a higher award."[129] If the higher award was ultimately disapproved, then the interim award became permanent. However, if the higher award was approved, the lower award had to be "revoked simultaneously" to avoid awarding two military decorations for the same act.[130] In this case, revocation was authorized purely to avoid running afoul of the 1926 executive order by President Coolidge, which stipulated that "[n]ot more than one of the several decorations authorized by Federal law will be awarded for the same act of heroism or extraordinary achievement."[131]

Revocation of previously presented decorations due to misconduct was first authorized in Army regulation in 1961, some fifty-eight years after the appearance of the "subsequent honorable service" provision in policy. The regulation specified that "[a]ny award for meritorious service may be revoked if facts subsequently determined would have prevented original approval of the award."[132] This was the first express authority for revocation of this type among any of the services in regulations issued after World War I. Curiously, the language went well beyond subsequent misconduct, as "facts subsequently determined" appears to reference misconduct either prior to or during a qualifying period of service. After all, subsequent misconduct would not "have prevented original approval," since this would require approving officials to have knowledge of the future. Notably, the scope of this provision was restricted to service medals, which was likely due to the inherent characteristics of this type of decoration; service medals are distinguishable from valor or achievement medals because they are often based on a protracted period of service rather than a discrete event.[133] Thus,

---

[129] U.S. DEP'T OF ARMY, REG. 672-5-1, DECORATIONS AND AWARDS 9 (20 July 1956).
[130] *Id.*
[131] Exec. Order No. 4601 (Mar. 1, 1927), *reprinted in* STAFF OF H. COMM. ON HOMELAND SEC., 111TH CONG., COMPILATION OF HOMELAND SECURITY RELATED EXECUTIVE ORDERS (E.O. 4601 THROUGH E.O. 13528) (1927–2009) 9 (Comm. Print 2010).
[132] U.S. DEP'T OF ARMY, REG. 672-5-1, AWARDS para. 17 (3 May 1961).
[133] *Compare id.*, *with* AR 600-8-22, *supra* note 30, para. 1-18*a*.

less-than-honorable actions during the qualifying period of service materially undermine a key qualification for the award in a way that they might not for a valor or achievement medal.

The Army subsequently revoked several decorations in high-profile cases during the 1960s, but they tended to be either awards for meritorious service or awards that were clearly fraudulent. One high-profile case was the first Sergeant Major of the Army, William O. Wooldridge, who was stripped of his Distinguished Service Medal in 1969 after he was implicated in a bribery scheme related to the operation of Service member clubs in Vietnam.[134] The Army released a statement that claimed that "information became available which established that he did not merit the award" without further elaboration.[135] Later, Wooldridge pleaded guilty to bribery, was ordered to sign over most of his assets to the Government, and was sentenced to five years of probation.[136] Also implicated in the same scandal was Major General Carl C. Turner, the former Provost Marshal General of the Army, who also saw his Distinguished Service Medal revoked.[137] In that case, the Army explained that "[Turner's] service for the period did not merit the award," clearly implying that misconduct had materially tarnished the period of qualifying service.[138]

A rare case of revocation of valor and achievement awards occurred in 1970, when it was discovered that fraud had tainted several medals awarded to Brigadier General Eugene P. Forrester, the assistant division commander of the First Cavalry Division. Specifically, at the end of Forrester's tour in Vietnam, the division's chief of staff, Colonel George Newman, discovered that Forrester had not been recommended for any awards. Newman directed his staff to draft award recommendations overnight, which led to narratives that were entirely falsified.[139] After an investigation, Forrester was ultimately stripped of both the Silver Star and the Distinguished Flying

---

[134] *Pentagon Revokes Service Decoration of Former Top G.I.*, N.Y. TIMES, Sept. 6, 1969, at 17.
[135] *Id.*
[136] *Ex-Top G.I. Gets Probation in Bribery*, N.Y. TIMES, May 30, 1973, at 36.
[137] *Turner Service Medal Revoked by the Army*, N.Y. TIMES, Oct. 9, 1969, at 53; *see Retired Army Gen. Carl C. Turner, 83, Dies*, N.Y. TIMES, Jan. 1, 1997 at B6 (documenting that Turner was later incarcerated in 1971 for tax evasion and stealing firearms).
[138] *Turner Service Medal Revoked by the Army*, *supra* note 137.
[139] *Army Begins Moving to Rescind General's Controversial Medal*, N.Y. TIMES, Oct. 27, 1970, at 12.

Cross.[140] What is noteworthy is that the medals were not revoked because of less-than-honorable conduct by the recipient, but rather because the actions actually cited for the awards were complete fabrications.

In 1974, Army regulation expanded misconduct-related revocation to include any personal decoration already presented, which included valor awards. The new regulation specified that "[o]nce an award has been presented, it may be revoked if facts subsequently determined would have prevented original approval of the award, had they been known at the time of award."[141] The addition of the language about facts preventing approval "had they been known at the time of the award" further clarified that the language was referencing the time before or during the qualifying period of service, not later service as with the "subsequent honorable service" provision. By 1980, the same regulation required a "statement of concurrence/nonconcurrence" from "the individual concerned."[142] In 1982, the regulation contained a provision about appellate options, explaining that "the affected individual will be informed that he/she may appeal the revocation action through command channels to [Headquarters, Department of the Army]."[143] These were clear attempts to ensure revocation was accompanied by notice and due process, in order to prevent successful legal challenges.

Due process related to medal revocation has perhaps become even more important in recent decades, as both Federal and State laws conferred substantial collateral property interests on recipients of military medals, particularly combat-related decorations. Medal of Honor recipients receive benefits the Army refers to as "entitlements," such as a special pension, air transportation, commissary and exchange privileges, and burial honors.[144] Enlisted recipients of Service Crosses or the Medal of Honor receive a ten percent increase in retired military pay.[145] The Federal Government offers enhanced veterans' preference in hiring to Purple Heart and campaign medal

---

[140] *U.S. Orders Medals Taken from General*, CHI. TRIB., Oct. 23, 1970, at 9.
[141] U.S. DEP'T OF ARMY, REG. 672-5-1, MILITARY AWARDS para. 1-28*a* (3 June 1974) (C4, 1 Aug. 1974).
[142] U.S. DEP'T OF ARMY, REG. 672-5-1, MILITARY AWARDS para. 1-28*a* (15 Dec. 1980) (C6, 15 Jan. 1981).
[143] U.S. DEP'T OF ARMY, REG. 672-5-1, MILITARY AWARDS para. 1-28*a* (1 Sept. 1982) (C7, 1 Oct. 1982).
[144] AR 600-8-22, *supra* note 30, para. 1-39.
[145] 10 U.S.C. § 3991(a)(2).

recipients.[146] Arlington National Cemetery allows interment of Medal of Honor, Service Cross, Distinguished Service Medal, Silver Star, and Purple Heart recipients who do not otherwise qualify for burial.[147] The military uses the Purple Heart as one basis for eligibility to combat-related special compensation, an entitlement that increases combat-related disability.[148]

In Alabama, public colleges may waive all undergraduate tuition and fees for Purple Heart recipients.[149] In Massachusetts, recipients of the Medal of Honor or a Service Cross are entitled to tax exemptions[150] and free vehicle license plates.[151] In New Hampshire, certain valor medals, campaign medals, and combat-related badges qualify recipients for a tax credit.[152] In Missouri, most valor medal recipients may park their vehicles for free at any public college or university in the state.[153] In Texas, recipients of valor medals and some service medals merit free license plates,[154] waiver of toll fees,[155] and waiver of most governmental parking fees.[156] In Golsteyn's residence of Virginia,[157] recipients of the Medal of Honor[158] or Purple Heart[159] receive free license plates and vehicle registration exemptions, and Medal of Honor recipients are not taxed on military retirement income.[160] These are just a few of the property interests that are indirectly conferred through these decorations.

---

[146] *Policy, Data, Oversight: Veterans Services*, U.S. OFF. OF PERS. MGMT., https://www.opm.gov/policy-data-oversight/veterans-services/vet-guide-for-hr-professionals (last visited Sept. 10, 2021).
[147] *Establishing Eligibility*, ARLINGTON NAT'L CEMETERY, www.arlingtoncemetery.mil/funerals/scheduling-a-funeral/establishing-eligibility (last visited Sept. 10, 2021).
[148] U.S. DEP'T OF DEF., COMBAT-RELATED SPECIAL COMPENSATION 5 (2004).
[149] ALA. CODE § 16-1-43 (2016).
[150] MASS GEN. LAWS ch. 90, § 2 (2021).
[151] *Id.* ch. 59, § 5.
[152] N.H. REV. STAT. ANN. § 72:28 (2018).
[153] MO. REV. STAT. § 304.725(1) (2017).
[154] TEX. TRANSP. CODE ANN. § 504.315 (2021).
[155] *Id.* § 372.053.
[156] *Id.* § 681.008.
[157] Lamothe, *supra* note 104.
[158] VA. CODE ANN. § 46.2-745 (2004).
[159] *Id.* § 46.2-742.
[160] *Id.* § 58.1-322.02(18).

D. Army Regulations Applied to Golsteyn and Subsequent Controversy

By the time Golsteyn's Silver Star was revoked in 2014, both the Army's regulation concerning revocation of decorations and its practice thereof had evolved considerably, even if the statutory authority had not. Army regulation authorized revocation after presentation "if facts subsequently determined would have prevented original approval of the award had they been known at the time,"[161] which clearly applied to Golsteyn's circumstances. The regulation further specified that presentation was "the physical act of pinning or clipping the medal on a Soldier's chest or handing the Soldier the medal, certificate or orders,"[162] which notably precluded Golsteyn from claiming that his Distinguished Service Cross was already presented. Further, the regulation gave express due process protections by requiring "a statement of concurrence or non-concurrence (with comments) from the individual concerned," as well as appeal options.[163]

It is perhaps unsurprising that when Golsteyn's medal was revoked, it sparked an outcry from some members of Congress who saw the move as outside of the military's authority. Representative Duncan Hunter, a member of the House Armed Services Committee, claimed that "once you allow for political appointees to take away something of which they know nothing whatsoever, you're politicizing the awards process."[164] In Hunter's view, "[t]here are probably people in jail now that are most proud of the one thing they did in their life. And it might have been on the battlefield . . . you can't take that away from them, no matter what they might have done afterwards."[165]

Former Secretary of the Army John McHugh justified the revocation to Hunter by citing that "facts subsequently determined" would have prevented the original approval.[166] In his view, if the U.S. Forces-Afghanistan

---

[161] U.S. DEP'T OF ARMY, REG. 600-8-22, MILITARY AWARDS para. 1-30*a* (11 Dec. 2006).
[162] *Id.*
[163] *Id.*
[164] Kyle Jahner, *Lawmakers Agree to Limit Power to Revoke Valor Awards*, ARMY TIMES (May 4, 2015), https://www.armytimes.com/news/your-army/2015/05/04/lawmakers-agree-to-limit-power-to-revoke-valor-awards.
[165] *Id.*
[166] Kyle Jahner, *Congressman Pushes Army on Why It Revoked Green Beret's Silver Star*, ARMY TIMES (Feb. 5, 2015), https://www.armytimes.com/news/your-army/2015/02/05/congressman-pushes-army-on-why-it-revoked-green-beret-s-silver-star.

commander—who had been delegated approval authority—had previously known about "the derogatory information" in Golsteyn's case, "he would not have awarded [him] the Silver Star."[167] McHugh also referenced the "subsequent honorable service" statutory provision, as well as the Department of Defense's *Manual of Military Decorations and Awards*, in stating that there would be no award of a medal to a Service member "whose entire service during or after the time of the distinguished act, achievement, or meritorious service has not been honorable."[168] Notably, the "subsequent honorable service" provision and the cited manual provision did not necessarily cover Golsteyn's case, since the Army tentatively concluded that his misconduct occurred before his qualifying service.[169] However, the Army's regulation certainly was applicable, as it clearly authorized revocation due to misconduct prior to medal qualification. It is also possible that McHugh referenced the requirement for honorable service before, during, and after qualification because of the uncertainty surrounding when Golsteyn's misconduct actually occurred.

Hunter was clearly unsatisfied with McHugh's explanation. In 2015, he sponsored legislation that sought to remove the military's authority to unilaterally "revoke any combat valor award."[170] The provision was incorporated into a version of the National Defense Authorization Act for Fiscal Year 2016, but was removed in conference.[171] Reportedly, there was ambivalence about the provision because it would have prevented military secretaries from making needed corrections, even in cases of fraud or mistake, as in the case of Brigadier General Forrester.

According to Representative Adam Smith, the provision would have impacted more than "just [Golsteyn's] individual case"; the provision "says under no circumstances once a service award is given can it be taken away."[172] Representative Joe Heck agreed, claiming that the provision sought to change "how awards are revoked not just in this case, but across

---

[167] *Id.*
[168] Larry Kummer, *How Does the Army Reward Heroism? Not Well, as This Story Shows*, FABIUS MAXIMUS (Feb. 7, 2015), https://fabiusmaximus.com/2015/02/07/us-army-matthew-golsteyn-hero-punished-dod-78310.
[169] *U.S. Army Documents on Major Mathew Golsteyn*, *supra* note 94.
[170] H.R. 2011, 114th Cong. (2015).
[171] H.R. REP. NO. 114-102 (2015).
[172] Jahner, *supra* note 164.

the board."[173] Hunter sponsored similar provisions that were incorporated into versions of the National Defense Authorization Acts for Fiscal Years 2018 and 2019, but they were also removed in conference.[174]

In 2019, the Office of the Secretary of Defense released new guidance on revocation limits, probably in reaction to Hunter's repeated attempts to curtail this authority. The guidance stated that

> [t]he revocation of [personal military decorations] under the "honorable" service requirement should be used sparingly and should be limited to those cases where the Service member's actions are not compatible with continued military service, result in criminal convictions, result in determinations that the Service member did not serve satisfactorily in a specific grade or position, or result in a discharge from military service that is characterized as "Other Than Honorable," "Bad Conduct," or "Dishonorable."[175]

This rationale apparently was based on the premise that separation should be the threshold for less-than-honorable service, since failure to separate implicitly labels the actions in question as honorable—or at least honorable enough to merit retention. It appears that the Office of the Secretary of Defense only intends for the provision to apply retroactively to members who are still under military jurisdiction or who committed offenses under military jurisdiction serious enough to recall them for courts-martial. However, this is merely a framework and is not necessarily present in service-level regulations.[176] Notably, this guidance would still sanction the revocation of Golsteyn's medal, since his actions resulted in a determination that he "did not serve satisfactorily in a specific grade or position."[177] The Office of the Secretary of Defense likely influenced subsequent legislation, enacted in December 2019, which expanded the "subsequent honorable

---

[173] *Id.*
[174] H.R. REP. NO. 114-404 (2017); H.R. REP. NO. 115-874 (2018).
[175] U.S. DEP'T OF DEF., INSTR. 1348.33, DOD MILITARY DECORATIONS AND AWARDS PROGRAM sec. 8 (Dec. 21, 2016) (C3, June 20, 2019) [hereinafter DODI 1348.33].
[176] *See* U.S. DEP'T OF DEF., INSTR. 5025.01, DOD ISSUANCES PROGRAM 17 (Aug. 1, 2016) (C3, May 22, 2019) (listing that Department of Defense instructions "[m]ay provide general procedures for implementing policy").
[177] DODI 1348.33, *supra* note 175.

service" provision to encompass all decorations issued in any military service.[178] This effectively gave stronger backing for revocation of many Army and Air Force medals, since the previous statutes requiring subsequent honorable service did not cover all military awards.[179]

E. Analysis of Authority Behind Regulations Applied to Golsteyn

There is certainly an argument that the authority to revoke Golsteyn's Silver Star was poorly linked to statutory authority, given the fact that the regulations implementing the "subsequent honorable service" provision have evolved considerably over the last century. There is also little doubt that the Army never intended to revoke awards in this manner when the authorizing statute was first enacted, evidenced by the facts that this express authority was completely absent in the regulations and that it was not exercised retroactively for many decades. Rather, until the 1960s, the Army likely intended known misconduct to prevent an award from being either approved or presented in the future—in the same manner as applied to Golsteyn when the Army revoked his medal's upgrade to the Distinguished Service Cross prior to presentation.

While the full scope of the Army's regulation on medal revocation may not be clearly traceable to a statute, this fact does not make it invalid. After all, the "subsequent honorable service" statute was itself a regulation for some fifteen years prior to codification, suggesting that the military has the independent authority to set the parameters of revocation in the absence of statutory restrictions to the contrary. This is also consistent with judicial interpretation of executive and congressional authority to regulate the military under the Constitution—the so-called military deference doctrine.[180] Under the modern version of this doctrine articulated in the 1970s, the Supreme Court recognized that the military is "a specialized society separate from civilian society" with its own "laws and traditions," including a greater ability to regulate conduct in view of this "different

---

[178] 10 U.S.C. § 1136.

[179] *See* Act of July 9, 1918, Pub. L. No. 65-193, 40 Stat. 845, 872; Act of July 2, 1926, Pub. L. No. 69-446, 41 Stat. 780, 789 (stipulating that these statutes requiring subsequent honorable service only covered the Medal of Honor, Distinguished Service Cross, Distinguished Service Medal, Soldier's Medal, and Distinguished Flying Cross).

[180] John F. O'Connor, *Statistics and the Military Deference Doctrine: A Response to Professor Lichtman*, 66 MD. L. REV. 668, 694 (2007).

relationship of the Government to members of the military."[181] In applying the doctrine, the Court has expressly endorsed "a healthy deference to legislative and executive judgments in the area of military affairs,"[182] and "great deference even when the President acts alone in [the areas of foreign and military affairs]."[183] Military awards and decorations are certainly a longstanding aspect of military culture, and they represent an import tool for incentivizing behavior and "improving morale" both on and off the battlefield.[184] Thus, the ability to award and revoke medals arguably falls squarely within this special relationship.

It is also notable that existing statutory authority to regulate honorable service does not specify that subsequent less-than-honorable service is the exclusive route to medal disqualification.[185] Revocation is also a possible interpretation of the requirement for honorable service—at least for subsequent misconduct, particularly since the provision does not clearly address whether a medal will simply be withheld or also revoked. The practice of medal revocation is also consistent with other consequences of misconduct, such as retroactive reduction of retirement rank to "the highest permanent grade in which [an officer] served on active duty satisfactorily."[186] As with medal revocation, reducing an officer to the last grade in which they served satisfactorily suggests that less-than-honorable service taints more than merely the period after misconduct. Also, as with medal revocation after presentation, reducing a retirement grade can be performed retroactively in cases where misconduct is discovered after officers already retired[187]—Army regulations allow reopening of retirement grades when a "separation and/or accompanying grade determination was procured by fraud,"[188] and also in cases when "[s]ubstantial new evidence [is] discovered after, contemporaneously with, or within a short time before separation [which] could result in a lower grade determination . . . ."[189] This standard is very much comparable to revocation of personal military

[181] Parker v. Levy, 417 U.S. 733, 743, 751 (1974).
[182] Rostker v. Goldberg, 453 U.S. 57, 66 (1981).
[183] Boumediene v. Bush, 553 U.S. 723, 832 (2008).
[184] U.S. DEP'T OF ARMY, THE MEDAL OF HONOR OF THE UNITED STATES ARMY 25 (1948).
[185] 10 U.S.C. § 1136.
[186] *Id.* § 1370(a)(1).
[187] *Id.*
[188] U.S. DEP'T OF ARMY, REG. 15-80, ARMY GRADE DETERMINATION REVIEW BOARD AND GRADE DETERMINATIONS para. 4-1*c*(1) (12 Feb. 2020).
[189] *Id.* para. 4-1*c*(2).

decorations based on "facts subsequently determined [which] would have prevented original approval of [an] award."[190] It is notable, however, that unlike many cases of medal revocation, retirement grade reduction is based in statute, not regulation.

F. Analysis of Golsteyn's ABCMR Application

In 2019, Golsteyn appealed to the ABCMR to reinstate his Distinguished Service Cross on the grounds that its revocation was an "unjust action" that contravened the Senior Army Decorations Board, as well as former president Trump's alleged promise that "everything would be expunged."[191] According to Golsteyn's counsel, "this is an easy fix that can be completed with a phone call and a signature for a deserving warrior."[192] The ABCMR disagreed, opining that Golsteyn "failed to demonstrate by a preponderance of evidence that an error or injustice occurred such that the applicant should be awarded either the DSC or the [Silver Star]."[193] Specifically, the ABCMR noted that Golsteyn's "overall behavior . . . did not indicate innocence," and that his "actions were not compatible with continued military service."[194] Further, though Golsteyn requested removal of the general officer memorandum of reprimand from his personnel file, the ABMCR declined, noting that the Department of Justice's acting pardon attorney had informed him that his pardon did "not erase or expunge the record of offense charges and does not indicate innocence,"[195] and that "it was not necessary, or even desirable, to expunge all records describing or condemning [his] now-pardoned conduct."[196]

Golsteyn's ABCMR case was unlikely to result in the reinstatement of his Distinguished Service Cross for the simple reason that such a correction is outside of the board's statutory authority. The decoration has a clear statute of limitations that requires awarding "within five years after the date of the act justifying the award,"[197] which had already expired in Golsteyn's case. Congress extended the statute of limitations for the review that

---

[190] AR 600-8-22, *supra* note 30, para. 1-30*a*.
[191] Mathew Golsteyn, No. AR20200000309, Army Bd. for Corr. of Mil. Records 1 (June 26, 2020).
[192] *Id.* at 2.
[193] *Id.* at 11.
[194] *Id.*
[195] *Id.* at 9.
[196] *Id.* at 13.
[197] 10 U.S.C. § 7274(b)(1).

recommended upgrading Golsteyn's medal, but this extension also expired in December 2019.[198] Thus, Golsteyn's request clearly fell under regulations as a case where the ABCMR "is not authorized to act for the Secretary of the Army," since neither the Secretary of the Army nor the President can award the medal on their own in violation of an act of Congress.[199] Such a request could have been recommended by the ABCMR, but implementation would have required both presidential approval and congressional waiver.[200]

It is notable that the ABCMR arguably possessed the authority to reinstate Golsteyn's interim Silver Star through its record correction power, as this medal is not constrained by a statute of limitations.[201] However, depending on when Golsteyn's misconduct occurred, restoring this medal might violate the statutory requirement for his subsequent service to be honorable—a status that remains unchanged by the pardon[202] or the regulatory authority to revoke a medal "if facts subsequently determined would have prevented original approval of the award had they been known at the time of approval."[203] Restoration of revoked awards is not unprecedented. The ABCMR has restored at least six revoked Medals of Honor in prior cases; however, the board acted without congressional waivers and in violation of other statutory requirements, making these restorations unlawful.[204] It is also possible that other restorations have occurred, but verification is difficult because the service boards for correction of military records (BCMRs) do not presently publish all decisions, as required by Federal law.[205]

Following the ABCMR's ruling, Golsteyn's attorney continued to lobby the President on Twitter to reverse the decision unilaterally, even

---

[198] National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 582(a), 130 Stat. 2000, 2149 (2016).
[199] U.S. DEP'T OF ARMY, REG. 15-185, ARMY BOARD FOR CORRECTION OF MILITARY RECORDS para. 2-13*b*(3) (31 Mar. 2006).
[200] MEARS, *supra* note 5, at 192.
[201] 10 U.S.C. § 7276; U.S. DEP'T OF WAR, *supra* note 67, sec. 105.
[202] 10 U.S.C. § 1136.
[203] AR 600-8-22, *supra* note 30, para. 1-30*a*.
[204] *See generally* MEARS, *supra* note 5, at 167–80 (discussing administrative restorations); Dwight S. Mears, *"Neither an Officer nor an Enlisted Man": Contract Surgeons' Eligibility for the Medal of Honor*, 85 J. MIL. HIST. 51, 60 (2021).
[205] 10 U.S.C. § 1552(a)(5); *NVLSP Appeals Dismissal of Its Lawsuit to Compel Pentagon to Post All DRB & BCMR Decisions*, NAT'L VETERANS LEGAL SERVS. PROGRAM (Apr. 14, 2020), https://www.nvlsp.org/news-and-events/press-releases/nvlsp-appeals-dismissal-of-its-lawsuit-to-compel-pentagon-to-post-all-drb-b.

though such an action likely would have been unlawful due to the statute of limitations governing the award.[206] The attorney claimed that allowing the revocation to stand amounted to "kowtow[ing]" to the officials who revoked Golsteyn's medal, allegedly as a political move.[207] He also urged the President to "[t]ake charge of the Army" by overruling the Secretary of the Army,[208] who he claimed "stole" Golsteyn's decoration.[209] This stance suggested the Army's personnel actions in Golsteyn's case were tainted by political motives, beyond its authority, or otherwise inconsistent with the President's pardon determination. However, the ABCMR record suggests that little or no evidence was offered to support these assertions.[210]

G. Analysis of Potential Administrative Procedure Act Claim in the Golsteyn Case

Since Golsteyn failed to have his medal reinstated by the ABCMR, he can file a lawsuit in Federal court seeking relief under the Administrative Procedure Act.[211] This merely requires a "final agency action" as a prerequisite, which could be either an ABCMR denial or a service-level denial that results in legal consequences.[212] The likelihood of success in court is slim because the burden of proof is extraordinarily high.

In 1983, the Supreme Court affirmed the standard of review for BCMR decisions in *Chappell v. Wallace*, holding that BCMR decisions "can be set aside if they are arbitrary, capricious or not based on substantial evidence."[213] In evaluating these factors, a court must consider whether agency decisions were made "on a consideration of the relevant factors and whether there has been a clear error of judgment."[214] Also, the reviewing

---

[206] 10 U.S.C. §7274(b)(1).
[207] @MilitaryDefendr, TWITTER (Dec. 23, 2020, 11:33 P.M.), https://twitter.com/MilitaryDefendr/status/1341965096948404225.
[208] @MilitaryDefendr, TWITTER (Dec. 18, 2020, 6:51 P.M.), https://twitter.com/MilitaryDefendr/status/1340082287023517696.
[209] @MilitaryDefendr, TWITTER (Dec. 17, 2020, 9:55 P.M.), https://twitter.com/MilitaryDefendr/status/1339766094437834753.
[210] *See generally* Mathew Golsteyn, No. AR20200000309, Army Bd. for Corr. of Mil. Records (June 26, 2020).
[211] 5 U.S.C. §§ 701–706.
[212] Bennett v. Spear, 520 U.S. 154, 178 (1997).
[213] Chappell v. Wallace, 462 U.S. 296, 303 (1983).
[214] Citizens to Pres. Overton Park v. Volpe, 401 U.S. 402, 416 (1971) (citing LOUIS L. JAFFE, JUDICIAL CONTROL OF ADMINISTRATIVE ACTION 182 (1965)).

court is deferential to the agency, and thus "is not empowered to substitute its judgment for that of the agency."[215]

Few plaintiffs have contested BCMR decisions affirming medal revocations—and almost none successfully, likely because of the high burden of proof involved under the Administrative Procedure Act and because revocation due to clear misconduct (or as a collateral consequence of conviction) leaves little to contest. Thus, most cases resulting in litigation are instances of retroactive revocation of service medals due to administrative punishment.[216] One such recent case, *Hoffler v. Hagel*, saw Lieutenant Colonel (Retired) Joseph Hoffler contest an Air Force BCMR (AFBCMR) refusal to reverse a letter of reprimand, lack of promotion, and retroactive revocation of a Meritorious Service Medal.[217] Hoffler claimed that the medal revocation was "a reprisal for his writing to his Senator," but the AFBCMR found that there was no "substantive evidence" to prove that the action "was an abuse of discretion, improper, or based on erroneous information."[218] The district court dismissed the complaint on summary judgment, holding that there was no evidence that the AFBCMR acted "arbitrarily or capriciously when it denied Hoffler's request for relief."[219] The denial was appealed to the United States Court of Appeals for the Fourth Circuit, where the court affirmed dismissal on the grounds that the appellant's arguments "as to why the revocation of his medal was improper . . . constitute no more than unsubstantiated speculation."[220] In sum, both courts correctly refused to substitute their judgment for that of the AFBCMR in the absence of proof of decision-making that was "arbitrary, capricious or not based on substantial evidence."[221]

Only once in history has a Federal judge returned a revoked valor decoration to a plaintiff in a lawsuit contesting a BCMR determination. In 1992, a district court directed the Secretary of the Navy (SECNAV) to return a Navy Cross to Alonzo Swann.[222] Swann, a steward's mate first

---

[215] *Id.*
[216] *See, e.g.*, Koster v. United States, 685 F.2d 407 (Ct. Cl. 1982); Hoffler v. Hagel, 122 F. Supp. 3d 438, 441 (E.D.N.C. 2015), *aff'd in part, dismissed in part sub nom.* Hoffler v. Mattis, 677 F. App'x 119 (4th Cir. 2017).
[217] *Hagel*, 122 F. Supp. at 441.
[218] *Id.*
[219] *Id.* at 447.
[220] *Mattis*, 677 F. App'x at 120.
[221] Chappell v. Wallace, 462 U.S. 296, 303 (1983).
[222] Swann v. Garrett, 811 F. Supp. 1336 (N.D. Ind. 1992).

class stationed in "Gun Tub #10" on the aircraft carrier *USS Intrepid* during World War II, had been presented the medal only to have it revoked and downgraded with no explanation.[223] When the carrier was attacked by a Japanese kamikaze aircraft, Swann remained at his post even after "it became apparent that the enemy plane was headed directly for his gun tub."[224] While several other gun crews on the carrier abandoned their positions to save themselves,[225] Swann "steadfastly continued to deliver effective gun fire upon the enemy until the Japanese plane crashed into the tub and exploded," injuring him and killing nine others.[226] Swann alleged that he was subsequently awarded and presented the Navy Cross, but that the medals given to him and other members of his gun tub were then "taken away and substituted with Bronze Stars because of their race."[227]

Swann made an application to the Navy's Board for Correction of Naval Records (BCNR) to request that the Navy Cross be reinstated, but the Navy replied that "[o]fficial Navy records do not show any evidence of the Navy Cross being awarded to [him]" and denied his request for relief on several occasions.[228] Strangely, the BCNR acknowledged that Swann was "issued a temporary citation for the Navy Cross," but claimed there was no clear evidence that race had influenced a downgrade of the award.[229] While it does not appear that the court fully understood the implications of revoking a valor award that was already presented, the fact of the prior presentation was included in the court's justification for reversing the decision.[230] The court ruled that the BCNR's decision was "not supported by substantial evidence in the record" due to numerous records, contemporaneous media reports demonstrating that the medals had in fact been awarded, and even a photograph of one of the gun tub crewmen receiving the Navy Cross.[231] In the court's opinion, failure to "correct blatant injustice in the record" meant that the BCNR acted in violation of its own mandate, and "thus arbitrarily or capriciously."[232] The court reasoned that "when an agency does not

---

[223] *Id.* at 1337.
[224] *Id.* at 1340.
[225] *Id.* at 1337.
[226] *Alonzo A. Swann*, HALL OF VALOR PROJECT, https://valor.militarytimes.com/hero/20995 (last visited Oct. 3, 2021).
[227] *Swann*, 811 F. Supp. at 1337.
[228] *Id.*
[229] *Id.* at 1338.
[230] *Id.* at 1343.
[231] *Id.* at 1340–42.
[232] *Id.* at 1340.

specify the factual or legal grounds for its decision, a court cannot give as much deference to the Board's determination."[233] Thus, the decision was reversed and remanded "with instructions to award Swann a Navy Cross."[234] Swann's case demonstrates why it is so rare for Federal courts to reverse determinations on military awards; the Government must utterly fail to justify its decision-making in order to make it arbitrary or capricious enough to overrule.

In light of these precedents, it is extremely unlikely that Golsteyn would prevail in Federal court. Army regulation expressly sanctions the post-presentation revocation of medals for misconduct, and the governing statute facially permits this action. Unlike in *Swann*, there is at least a rational basis for the Army's regulations and its adjudication in Golsteyn's case, meaning that they should survive minimum scrutiny and would not be deemed "arbitrary, capricious or not based on substantial evidence."[235]

Golsteyn's attorney has argued that the pardon has the effect of erasing misconduct as if it never occurred, but this claim is refuted by longstanding case law. As already discussed in the Lorance case study and Golsteyn's ABCMR case, the Justice Department's own position is that a pardon neither restores an individual's entitlements as if the offense had never occurred nor automatically results in expungement of records. Denial or revocation of medals due to misconduct is a matter internal to regulation of the military and does not constitute judicial punishment, so it is not impacted by a pardon. It is unclear if former president Trump actually ordered that Golsteyn's records be expunged separately from the pardon. If this happened and was actually enforced, it would potentially violate Federal record retention statutes that either require preservation or prohibit unsanctioned removal or destruction of records.[236]

Golsteyn may also argue that the Secretary of the Army improperly revoked his medal on the basis of the reprimand alleging a law of armed conflict violation, as the board of inquiry found that this allegation was unsubstantiated.[237] While these adjudications are inconsistent at some level,

---

[233] *Id.* at 1342 (citing Werner v. United States, 642 F.2d 404 (Ct. Cl. 1981)).
[234] *Id.* at 1343.
[235] Chappell v. Wallace, 462 U.S. 296, 303 (1983).
[236] 44 U.S.C. § 3106; 18 U.S.C. § 2071; 28 U.S.C. § 534(a)(1).
[237] Mathew Golsteyn, No. AR20200000309, Army Bd. for Corr. of Mil. Records 7 (June 26, 2020).

the board of inquiry still found that Golsteyn's actions met the threshold of conduct unbecoming an officer,[238] which the *Manual for Courts Martial* explains is

> action or behavior in an official capacity which, in dishonoring or disgracing the person as an officer, seriously compromises the officer's character as a gentleman, or action or behavior in an unofficial or private capacity which, in dishonoring or disgracing the officer personally, seriously compromises the person's standing as an officer.[239]

The board determined that Golsteyn committed "misconduct, moral, or professional dereliction," evidenced by its finding that he engaged in conduct unbecoming an officer, and recommended a characterization of service less than honorable.[240] It could certainly be argued that conduct unbecoming is less dishonorable than murder, but it is no less prejudicial when it comes to an already settled basis for medal revocation that warrants separation. Further, Golsteyn's televised admission to killing the suspect and acceptance of an unconditional pardon were both forms of admission that further support the board's determination that Golsteyn's service was less than honorable.

H. Overall Impact of Golsteyn Pardon and Recommendations

Overall, Golsteyn's case study illustrates that existing Army regulations and Federal statutes convey adequate authority to revoke medals in cases of subsequently determined misconduct. However, it also conveys that previous Army regulations on medal revocation have reversed themselves and The Judge Advocate General's precedent over the last century with no public explanation, and that modern regulations still lack clarity on the source of their authority. Given this history, it would be prudent to broaden the statutory language to include current regulations on revocation, if only to make this authority more clear. For example, Congress could amend the statute to clarify that revocation is also permissible when misconduct taints the qualifying period of service. The Air Force began to adopt this approach

---

[238] UCMJ art. 133 (1950).
[239] MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶ 90c(2) (2019).
[240] Mathew Golsteyn, No. AR20200000309, Army Bd. for Corr. of Mil. Records 7 (June 26, 2020).

in the 1960s, when its awards manual prohibited decorations when an Airman's "entire service during or subsequent to the time of the distinguished act, achievement, or service will not have been honorable."[241] Notably, that provision was, and is, purely regulatory, since the Air Force draws on the same statutory authority as the Army for the purposes of many of its military decorations, including the "subsequent honorable service" provision. One drawback of this proposal is that it may not cover circumstances like Golsteyn's, depending on whether his misconduct truly predated his qualifying period of service. However, it is arguable that Golsteyn's apparent actions should presumptively fall within the scope of this proposal, given that he admitted to misconduct, and thus should not benefit from the Government's inability to fix a precise date. Further, the conspiracy to burn the evidence and obstruct the investigation clearly postdated the killing, which certainly tainted the general time period of his gallant conduct if not the qualifying action itself.

Another issue highlighted by the Golsteyn case is the lack of time constraints on revocation, either in terms of time elapsed since the commission of misconduct or the temporal proximity of award qualification to a given period of misconduct. While Golsteyn's misconduct was first investigated less than two years after the incident,[242] it is clear that his own admission to the Central Intelligence Agency is the only reason that the Army discovered and investigated the alleged crimes. Thus, it is not unreasonable to speculate that absent this admission, the misconduct might otherwise have gone undiscovered for quite some time, if at all. Along these lines, if Golsteyn's misconduct were alternatively discovered after he had retired from a decades-long career, prosecution could theoretically result in revocation of all subsequent awards and decorations, possibly even other valor awards, including those earned decades after his misconduct. While present regulations would technically permit this outcome, such a broad application does not appear to have ever occurred. This scenario, however implausible, highlights that the ability to revoke awards for less-than-honorable service presently has no temporal limitation or requirement to be linked to the misconduct itself. While it may be impractical to tie the military's hands by enacting a statutory time limitation, it would be proactive for the Department of Defense to further refine its revocation

---

[241] 32 C.F.R. § 882.4 (Oct. 6, 1964); *accord* U.S. DEP'T OF AIR FORCE, REG. 900-10C, SERVICE AWARDS para. 4(b) (20 July 1961) (C, 14 Oct. 1964).
[242] *U.S. Army Documents on Major Mathew Golsteyn*, *supra* note 94.

guideline to ensure that the practice is both equitable and standardized among the military services. Such a guideline might sanction revocation of medals only if earned during the same grade, position, assignment, or tour tainted by misconduct. This would draw a clear distinction between medals tainted by temporal proximity to misconduct—as in Golsteyn's case—and those that might be separated by years of otherwise honorable service and have no identifiable nexus to misconduct.

V. Edward Gallagher and Revocation of Achievement Medals

A. Background

Edward Gallagher, a now-retired chief petty officer in the Navy's Sea, Air, and Land (SEAL) teams, was charged in September 2018 with the premeditated murder of an Islamic State captive, attempted murder of unarmed civilians, posing with the corpse of a deceased combatant, and other criminal offenses.[243] He was acquitted of murder and attempted murder, likely the result of a key witness contradicting his own prior statements and claiming responsibility for the killing after receiving immunity.[244] Gallagher was ultimately convicted of wrongfully posing for an unofficial picture with a human casualty, for which he was sentenced to four months' confinement (which he served in pretrial confinement) and a demotion of one grade.[245] Following this conviction, former president Trump ordered the demotion reversed.[246] When Gallagher made contemptuous remarks about senior Navy officials, the service ordered a review board to consider revoking his SEAL trident insignia.[247] Then-

---

[243] *Issuing Several Pardons, President Trump Intervenes in Proceedings of U.S. Troops Charged or Convicted of Acts Amounting to War Crimes*, 114 AM. J. INT'L L. 307, 309 (2020).

[244] Dave Philipps, *Navy SEAL Whose Testimony Roiled War-Crimes Trial May Face Perjury Charge*, N.Y. TIMES (June 26, 2019), https://www.nytimes.com/2019/06/26/us/corey-scott-edward-gallagher-navy-seal.html.

[245] Dave Philipps, *Navy SEAL Chief Accused of War Crimes is Found Not Guilty of Murder*, N.Y. TIMES (July 2, 2019), https://www.nytimes.com/2019/07/02/us/navy-seal-trial-verdict.html.

[246] *Statement from the Press Secretary*, *supra* note 33.

[247] Dave Philipps et al., *Trump's Intervention in SEALs Case Tests Pentagon's Intolerance*, N.Y. TIMES (Nov. 30, 2019), https://www.nytimes.com/2019/11/30/us/politics/trump-seals-eddie-gallagher.html.

President Trump intervened again by ordering that the pin not be revoked, sparking a dispute that led to the firing of SECNAV.[248]

The President clearly opposed the post-trial award of Navy Achievement Medals (also known as Navy and Marine Corps Achievement Medals) to several members of the team that prosecuted Gallagher.[249] While the attorneys in question had not been punished for any misconduct, the lead prosecutor was previously removed from the case for emailing an unauthorized tracking program to Gallagher's defense attorneys, allegedly in an attempt to combat leaks to the media.[250] Upon discovery of the decorations in July 2019, then-President Trump tweeted that the medals were "ridiculously given" to the prosecutors, claiming that "[n]ot only did they lose the case, they had difficulty with respect to information that may have been obtained from opposing lawyers and for giving immunity in a totally incompetent fashion."[251]

For this reason, former president Trump announced that he had "directed the Secretary of the Navy Richard Spencer & Chief of Naval Operations John Richardson to immediately withdraw and rescind the awards."[252] A Navy spokesman then made the claim that this action was within the secretary's authority and confirmed that the awards were immediately rescinded.[253] This unprecedented presidential intervention in a military justice case raises questions about whether revocation of military awards is lawful after awarding and presentation, particularly where the basis for revocation is a disagreement about the original award decision and the impacted Service members apparently received no notice or due process prior to revocation. Since the Navy's regulations lack any measurable

---

[248] Myers & Prine, *supra* note 3.

[249] Hope Hodge Seck, *Trump Orders Navy to Rescind Medals Given to SEAL Eddie Gallagher's Prosecutors*, MILITARY.COM (July 31, 2019), https://www.military.com/daily-news/2019/07/31/trump-orders-navy-rescind-medals-given-seal-eddie-gallaghers-prosecutors.html.

[250] Howard Altman, *Lead Navy Prosecutor in SEAL War Crime Case out over Email Spying*, NAVY TIMES (June 3, 2019), https://www.navytimes.com/news/2019/06/04/lead-navy-prosecutor-in-seal-war-crime-case-out-over-email-spying.

[251] Carl Prine, *Trump Nixes NAMs for 4 Prosecutors Tied to SEAL Case*, NAVY TIMES (July 31, 2019), https://www.navytimes.com/news/your-navy/2019/07/31/trump-nixes-nams-for-4-prosecutors-tied-to-seal-case.

[252] *Id.*

[253] Jeremy Diamond & Barbara Starr, *Trump Moves to Rescind Medals Awarded to Eddie Gallagher Prosecutors*, CNN (July 31, 2019), https://www.cnn.com/2019/07/31/politics/trump-rescinds-navy-prosecutors-medals/index.html.

criteria for revocation, are inconsistent with Department of Defense policy, and have already produced outcomes that are arguably arbitrary or capricious, it is likely that they could be overturned in either administrative or judicial forums.

B. History of Navy's Honorable Service Requirement

For much of the twentieth century, the Navy had a "subsequent honorable service" provision that differed from the Army's, owing to the fact that its statutes authorizing decorations were separate from the Army's. As discussed earlier, its "subsequent honorable service" provision was first passed by Congress in 1919, in a bill that contained military award provisions borrowed from the Army.[254] The primary difference was that the Navy's provision covered all future military decorations and insignia issued for that service, while the Army's covered only the decorations authorized in the bill itself. It is also notable that the Navy previously had a separate and longstanding practice of unilaterally revoking Medals of Honor for severe offenses such as desertion, although this was the product of prior regulations that were clearly superseded by the time of the 1919 legislation's enactment.[255]

In the twentieth century, the Navy did not expressly endorse retroactive revocation of medals as early as the Army. The Navy's first mention of any revocation authority appeared in its 1976 award regulations, which provided that "[a]ny award for a distinguished act, achievement, or service may be revoked before presentation if facts subsequently determined would have prevented original approval of the award."[256] Here, by implication, the Navy saw revocation under this provision as impermissible if it occurred after presentation—a key difference from the Army's regulations of the same period. It is clear that the Navy saw presentation as a key step that would limit the ability to revoke a medal, since presentation is the point where legal rights to the medal vest.

In 1991, the Navy added regulatory language suggesting that revocation after presentation was possible at a higher level. The new regulation instructed that "[i]f the awardee's honorable service is questioned after

---

[254] MEARS, *supra* note 5, at 74; Act of Feb. 4, 1919, Pub. L. No. 65-253, 40 Stat. 1056, 1057.
[255] MEARS, *supra* note 5, at 17.
[256] U.S. DEP'T OF NAVY, SEC'Y OF NAVY INSTR. 1650.1E, NAVY AND MARINE CORPS AWARDS MANUAL sec. 7(b) (17 Nov. 1976) [hereinafter SECNAVINST 1650.1E].

presentation of the award, forward the entire case to the Navy Department Board of Decorations and Medals (NDBDM) . . . for a determination and final disposition."[257] Regulations published in 2002 expressly endorsed post-presentation revocation but reserved the authority for this action to SECNAV:

> Any award for a distinguished act, achievement or service may be revoked before presentation by the approval authority, or after presentation by SECNAV, if facts, subsequently determined, would have prevented the original approval of the award, or if the awardee's service after the distinguishing act, achievement or service has not been honorable.[258]

The wording was revised slightly in 2006 to state that "[i]f subsequently determined facts would have prevented the original approval of the award, or if the awardee's service after the presentation of the award has not been honorable, SECNAV may revoke the award."[259] The language pertaining to "facts, subsequently determined" in these regulations was clearly borrowed from the Army, which had developed revocation policies well before the Navy.

In May 2019, the Navy's regulations were revised again to clarify that "[a]fter any [personal military decoration], [Purple Heart], or unit decoration has been presented, SECNAV is the sole authority for revocation."[260] No criteria were listed to specify what would merit revocation for personal military decorations. Also notable was lack of any due process protections in the Navy's regulations, such as the right to submit a non-concurring statement or an appeal.

Surprisingly, contemporaneous Department of Defense criteria continued to list that Defense and Joint medals awarded at this higher level

---

[257] U.S. DEP'T OF NAVY, SEC'Y OF NAVY INSTR. 1650.1F, NAVY AND MARINE CORPS AWARDS MANUAL sec. 115(3) (8 Aug. 1991) (C1, 25 Feb. 1992).
[258] U.S. DEP'T OF NAVY, SEC'Y OF NAVY INSTR. 1650.1G, NAVY AND MARINE CORPS AWARDS MANUAL sec. 116(2) (7 Jan. 2002).
[259] U.S. DEP'T OF NAVY, SEC'Y OF NAVY INSTR. 1650.1H, NAVY AND MARINE CORPS AWARDS MANUAL sec. 211(8)(b) (22 Aug. 2006) [hereinafter SECNAVINST 1650.1H].
[260] U.S. DEP'T OF NAVY, SEC'Y OF NAVY INSTR. 1650.1J, DEPARTMENT OF THE NAVY MILITARY AWARDS POLICY para. 5(k)(2) (29 May 2019) [hereinafter SECNAVINST 1650.1J].

could only be revoked "if facts, later determined, would have prevented original approval of the decoration."[261] The Department of Defense expanded its guidance on medal revocation in June 2019 to specify that personal military decorations, including those awarded by the Navy, "should be revoked if subsequently determined facts would have prevented the original approval or presentation of the award," and "should be limited to those cases where the Service member's actions are not compatible with continued military service."[262] Therefore, while the Navy's criteria for revocation did not textually contradict the Department of Defense guidance, the Navy's regulation notably failed to articulate a policy that implemented the clear limitations present in this higher policy.

Thus, at the time of the prosecutors' medal revocations in July 2019, the Army and the Navy had similar statutory authority governing honorable service requirements for medals. However, the Navy's regulations diverged from Army and Department of Defense regulations due to their complete absence of circumstances justifying revocation, and the lack of clear due process protections.

C. Analysis of Award Revocations in the Gallagher Case

When former president Trump ordered the revocation of the Navy Achievement Medals for the Gallagher prosecution team in July 2019, the Navy's then-current regulation specified that the medal "may be authorized for meritorious service or achievement in a combat or non-combat situation, based on sustained performance or specific achievement of a superlative nature, and shall be of such merit as to warrant more tangible recognition than is possible by a fitness report or performance evaluation."[263] Thus, the eligibility criteria were open-ended, and the medals could be awarded based primarily on the subjective judgment of the approval authority.

Media reports indicate that one revoked award was justified on the basis of "superior performance" in trial preparation, having "brilliantly cross-examined defense witnesses" and having "expertly delivered the

---

[261] U.S. DEP'T OF DEF., INSTR. 1348.33, MANUAL OF MILITARY DECORATIONS AND AWARDS: GENERAL INFORMATION, MEDAL OF HONOR, AND DEFENSE/JOINT DECORATIONS AND AWARDS vol. 1, para. 4(e)(8) (Nov. 23, 2010) (C3, July 10, 2014).
[262] DODI 1348.33, *supra* note 175.
[263] SECNAVINST 1650.1H, *supra* note 259, para. 13(b).

government's case in rebuttal."[264] Another revoked award cited "superior performance," "brilliant legal acumen," and the "unforeseen personnel change" that forced the attorney to become the lead prosecutor.[265] While the citations' authors may have interpreted these actions more favorably than others, it is unlikely that the awards' bases were materially falsified or objectively incorrect. Thus, it was unclear how the revocation decision was justified, since the Navy regulations stated that SECNAV was the "sole authority for revocation."[266]

The most glaring problems with the revoked achievement medals were the justifications invoked by former president Trump. Namely, he cited the prosecution's loss of the case, issues with information obtained during trial, and the botched immunity deal.[267] These claims are troubling not because they were untrue, but because they were known at the time of the awards' approval and presentation, which occurred several weeks earlier.[268] Further, the lead prosecutor had already been removed from the case, so he presumably did not receive an award because of the allegation of misconduct.[269] In other words, justifications seemingly failed to meet the Navy's previous threshold of being "subsequently determined facts [that] would have prevented the original approval of the award," a requirement that was still in force within the Department of Defense.[270] The stated grievances were not "subsequently determined facts" since the approval authorities certainly knew of them prior to their decision. Rather, it appears that the former president merely disagreed with the decision to award the medals, which had no other obvious basis for revocation such as fraud or material error.

While the Navy's regulations did not define what revocation threshold should be used, they also did not specify that revocation was permissible for any reason and, in this sense, were inconsistent with higher regulations. There is no question that the President or SECNAV could have lawfully

---

[264] Carl Prine, *Their Case Collapsed in Court but 4 Navy Prosecutors Still Netted NAMs*, NAVY TIMES (July 30, 2019), https://www.navytimes.com/news/your-navy/2019/07/30/their-case-collapsed-in-court-but-4-navy-prosecutors-still-netted-nams.
[265] *Id.*
[266] SECNAVINST 1650.1J, *supra* note 260.
[267] Seck, *supra* note 249.
[268] Prine, *supra* note 251.
[269] *Id.*
[270] *Compare* SECNAVINST 1650.1H, *supra* note 259, *with* DODI 1348.33, *supra* note 175.

intervened to prevent the awarding of the medals before presentation, but revocation after presentation has long been constrained by both policy and law. The Navy apparently interpreted this provision as granting authority to revoke an award for any reason, in direct contrast to earlier standing policy between 2002 and 2019 and contemporaneous Department of Defense regulations.

Also problematic was the fact that the Navy appeared to comply with the presidential directive almost instantaneously, which means that the impacted prosecutors would have had little to no opportunity to contest the decision.[271] Considering that the rights to these medals vested upon presentation several weeks earlier, this raises questions about due process, such as whether the impacted officers were afforded hearings or the ability to refute allegations prior to an adjudication with legal consequences. While there may have been subsequent administrative remedies, it is unclear if these were offered, and the extraordinary nature of the revocation directive would virtually guarantee that an appeal would be denied. After all, it is evident that Navy officials faced the option of either complying with the President's order or being removed. It is not farfetched to posit that any executive official reviewing the decision on appeal would face a similar conundrum.

Curiously, the Navy dramatically expanded its ability to revoke decorations only two weeks after the presidentially directed revocation of the achievement medals. The new regulation stated that "[i]n all cases, SECNAV retains the authority to revoke or downgrade any award after approval or presentation if, in the judgment of the Secretary, the individual or unit did not merit the award, or if it is otherwise in the best interests of the Navy."[272] It appears that the Navy has claimed authority to revoke awards unilaterally after presentation based solely on the subjective determination that the decision is "in the best interests of the Navy"—a remarkably open-ended clause. This language is far more expansive than any revocation regulation promulgated by any service in the twentieth century, and arguably allows revocation for virtually any reason.

---

[271] Prine, *supra* note 251.

[272] U.S. DEP'T OF NAVY, SEC'Y OF NAVY MANUAL M-1650.1, NAVY AND MARINE CORPS AWARDS MANUAL para. 1.2(f)(6) (16 Aug. 2019).

Notably, the Navy's present revocation authority was not in force at the time of former president Trump's directive to revoke the medals, although the expanded authority was likely a reaction to the absence of guidance in this very situation. It is quite possible that the President's intervention caused the service to review its award regulations, resulting in the discovery that they were silent on how a determination to revoke medals would be made. If this was the case, the expanded authority was perhaps an attempt to strengthen the regulation in order to counter administrative or legal challenges. However, since the regulation is inconsistent with equivalent Army[273] and Air Force[274] regulations, as well as higher Department of Defense policy,[275] it is more likely that the policy revision will produce the opposite outcome.

It is most problematic that the Navy's expanded regulations contradict the Office of the Secretary of Defense's June 2019 guidance, which had been issued less than two months earlier.[276] As these instructions were issued under the authority of the Under Secretary of Defense for Personnel and Readiness, the policy proponent had the express authority to "implement policy approved by the Secretary of Defense," including "instructions to the Military Departments."[277] In this case, the instructions specified that revocation of personal military decorations after presentation should only be exercised in

> cases where the Service member's actions are not compatible with continued military service, result in criminal convictions, result in determinations that the Service member did not serve satisfactorily in a specific grade or position, or result in a discharge from military service that is characterized as "Other Than Honorable," "Bad Conduct," or "Dishonorable."[278]

---

[273] AR 600-8-22, *supra* note 30.
[274] U.S. DEP'T OF AIR FORCE, MANUAL 36-2806, AWARDS AND MEMORIALIZATION PROGRAM attach. A, para. A4.6 (10 June 2019) [hereinafter AFMAN 36-2806].
[275] DODI 1348.33, *supra* note 175.
[276] *Id.*
[277] U.S. DEP'T OF DEF., DIR. 5124.02, UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS para. 6.4 (June 23, 2008).
[278] DODI 1348.33, *supra* note 175.

It appears that none of these circumstances applied to the prosecutors in question, as there is no evidence that they were accused of or flagged for misconduct.

D. Potential BCNR Remedy for Award Revocations in the Gallagher Case

Due to the conflicting regulations and dubious justification behind the revocation, the impacted Navy prosecutors have an excellent chance of contesting this decision at the BCNR. The decision would fall within the BCNR's purview, as it appears to be an injustice within the BCNR's mandate to "correct an error or remove an injustice."[279] Further, the Navy Achievement Medal is not a statutory medal and is thus not governed by a statute of limitations.[280] This means that it is squarely within SECNAV's authority to award and that, by extension, it is also within the BCNR's authority, as the BCNR exercises SECNAV's authority.[281] In making their case, the applicants could argue that the decision constituted undue command influence where lower regulations did not specify the grounds for revocation and higher regulations were willfully ignored.

E. Potential Administrative Procedure Act Claim for Award Revocations in the Gallagher Case

If the BCNR fails to reverse the decision, Federal court would be another potential avenue for relief. As discussed in the Golsteyn case study,[282] Federal courts can set aside BCMR decision "if they are arbitrary, capricious or not based on substantial evidence."[283] In *Swann v. Garrett*, the plaintiff met this burden by demonstrating that the BCNR had rejected a request for an award's reinstatement despite clear evidence that the medal had been both awarded and presented and later summarily revoked and downgraded with no clear explanation.[284] In the prosecutors' case, the plaintiffs could potentially satisfy this burden of proof by arguing that the President and SECNAV exceeded regulatory authority. Their case would

---

[279] 10 U.S.C. § 1552(a)(1).
[280] SECNAVINST 1650.1H, *supra* note 259, sec. 230(13)(b); *see* 10 U.S.C. § 1552(b) (stipulating that boards for correction of military records itself has a three-year statute of limitations from discovery of the error or injustice and that this may be excused "in the interest of justice").
[281] 10 U.S.C. § 1552(a)(1).
[282] *See* discussion *supra* Part IV.
[283] Chappell v. Wallace, 462 U.S. 296, 303 (1983).
[284] Swann v. Garrett, 811 F. Supp. 1336 (N.D. Ind. 1992).

be stronger than Golsteyn's because they could correctly claim that there was no subsequently discovered misconduct on which to base the revocation. In contrast, the Government would have difficulty refuting this argument, as former president Trump prominently documented his reasons for the revocation on Twitter.[285] The President's criticisms failed to satisfy any previous criteria for revocation, and appeared to be no more than disagreement in hindsight. The Navy could claim that the regulation allowed any justification for revocation, including a political motive, but the regulation notably failed to specify any criteria for such a decision. The Navy might also argue that the medal was revoked on grounds separate from the President's order, but this argument would likely be seen as pretextual.

F. Overall Impact of Award Revocations in the Gallagher Case and Recommendations

Overall, the revocations of military awards related to the Gallagher prosecution team illustrate that present regulations governing revocation are inadequate in several respects. First, the Navy's regulations contradict the regulations of the other services[286] and the Office of the Secretary of Defense[287] relating to the authority and criteria to revoke personal military decorations that were previously presented. Indeed, the Navy's most recent regulations on revocation are even incompatible with the overwhelming majority of the service's own prior regulations since revocation was first authorized by implication in 1976.[288] This suggests that there are competing views within the military establishment about the wisdom of unrestrained revocation, perhaps because this makes it more likely that the regulations will be successfully challenged, that Congress will impose its own limitations on revocation, or both.

While the Navy regulation's broad scope and ambiguity do not necessarily make it unlawful, it is insufficiently tied to misconduct—or any measureable standard—to protect Sailors from politically motivated revocation. By failing to articulate any clear standard for revocation, the Navy risks future political intervention as well as damage to the prestige of

---

[285] *E.g.*, Peter Baker, *Trump Orders Navy to Strip Medals from Prosecutors in War Crimes Trial* (July 31, 2019), https://www.nytimes.com/2019/07/31/us/politics/trump-navy-seal-war-crimes.html.
[286] AR 600-8-22, *supra* note 30; AFMAN 36-2806, *supra* note 274.
[287] DODI 1348.33, *supra* note 175.
[288] SECNAVINST 1650.1E, *supra* note 256.

the award system itself. After all, if decorations are revoked arbitrarily, capriciously, and without clear explanation, it will undoubtedly reduce their perceived value and any corresponding incentive for Sailors to earn them.

To put regulatory revocation provisions on a firmer legal footing, the Navy should, at a minimum, revert to the policy it utilized between 2006 and 2019, which articulated that revocation is permissible "[i]f subsequently determined facts would have prevented the original approval of the award, or if the awardee's service after the presentation of the award has not been honorable."[289] Further, it should adopt the policy of the Office of the Secretary of Defense and clarify the threshold when revocation is permissible for less-than-honorable service, such as

> cases where the Service member's actions are not compatible with continued military service . . . , result in criminal convictions, result in determinations that the Service member did not serve satisfactorily in a specific grade or position, or result in a discharge from military service that is characterized as "Other Than Honorable," "Bad Conduct," or "Dishonorable."[290]

Finally, the Navy should provide notice of procedures that afford Sailors greater due process in the case of proposed revocation—such as the ability to request a hearing, present counterevidence, and pursue an appeal.

VI. Conclusion

The authority to authorize a military decoration goes hand in hand with the ability to revoke the same, at least absent statutory restrictions. This means that in cases like those of Clint Lorance and Mathew Golsteyn, revocation is presumptively lawful. Lorance's case study is the least controversial, demonstrating that service medals can be forfeited by less-than-honorable conduct during a medal's qualifying period. Given that honorable service is a baseline requirement for a campaign medal, withholding the medal after serious misconduct during the qualifying period is not surprising. When administrative revocation of a medal accompanies a court-martial conviction, this determination is clear-cut. An unconditional pardon does little to change this outcome, as legal challenges, the

---

[289] SECNAVINST 1650.1H, *supra* note 259.
[290] DoDI 1348.33, *supra* note 175.

Department of Justice, and administrative precedent demonstrate that clemency restores rights and remits punishment but does not expunge records of misconduct or alter eligibility for military awards.

Golsteyn's case study is more complex due to the type of medal at issue, the uncertain timing of his misconduct, and the complicated history of regulations governing revocation of medals after presentation. Golsteyn qualified for a different type of military decoration than Lorance: a valor award, which is based more on a discrete act of heroism than a protracted period of service. Therefore, it is easier to argue that it remains untainted by misconduct, particularly since Golsteyn may have committed misconduct before, rather than during or after, his qualification. Had this scenario occurred in earlier twentieth century conflicts, it is possible that Golsteyn would have retained his medal irrespective of later investigations or prosecution, since Army regulation did not expressly sanction post-presentation revocation of valor awards due to misconduct until 1974.[291]

The regulatory authority for revocation in cases of pre-qualification misconduct is not based in statute and has evolved considerably since its inception, but has never been successfully challenged. Thus, Golsteyn's request to reinstate his decoration was denied by the ABCMR and would likely suffer similar rejection in Federal court since the Army's regulation covers his situation and is presumptively lawful. Nevertheless, the military would be wise to request that the governing statute be clarified, if only to make this authority less equivocal. Such an amendment might expressly require honorable service both during and after qualifying periods as a prerequisite for any medal. A regulatory guideline to tie medal revocation to the same general time period tainted by less-than-honorable conduct is also advisable to ensure that revocation is adequately linked to less-than-honorable conduct as well as standardized.

The revocation of achievement medals awarded and presented to the Gallagher prosecutors is more questionable than the Lorance and Golsteyn case studies due to the seemingly arbitrary justification, the Navy's inexplicable removal of regulatory standards for revocation in direct contrast with Department of Defense regulations, and the apparent lack of due process accompanying the determination. Regardless of whether the

---

[291] U.S. DEP'T OF ARMY, REG. 672-5-1, MILITARY AWARDS para. 1-28*a* (June 3, 1974), (C4, 1 Aug. 1974).

former president's disagreements were subjectively valid, it appears that there was no objective defect in the original award justifications, and he did not intervene until after the medals were presented. This sets a chilling precedent for medal revocation. If allowed to stand, it means that revocation can be accomplished without any rational justification, and would effectively be immune from any challenge due to the lack of measurable criteria.

Medals that were earned under well-defined eligibility criteria deserve equally clear criteria for revocation and the opportunity to contest proposed revocation. Otherwise, other medals associated with property rights may be revoked without notice and in violation of due process requirements. It should be possible to contest these revocations as arbitrary and capricious at the BCNR or Federal court, as the regulation seems to have granted impermissible discretion to SECNAV in apparent contrast to Department of Defense policy. At a minimum, the Navy's revocation provisions should be reverted to the prior version that corresponded with both the Department of Defense and the other military services. This would make revocation permissible only if subsequent facts demonstrate that the medal was not earned and that the misconduct was not compatible with continued military service.

THE THIRTY-SEVENTH CHARLES L. DECKER LECTURE IN ADMINISTRATIVE AND CIVIL LAW:* MILITARY LAW IN UNCERTAIN TIMES

EDWIN MEESE III†

General Huston, distinguished guests, ladies, and gentlemen, it is a great pleasure to be with you here and to have the honor of presenting the Decker Lecture. It is indeed a great privilege to be here.

I have known about The Judge Advocate General's Legal Center and School for quite some time. When I was a law professor before going into the Federal Government service, I was on the faculty and a professor of law at the University of San Diego, and our dean was a judge advocate himself. He did his annual duty for training by coming here. We on the faculty always knew when he was about to go on active duty because he shaved his beard.

It is a particular honor to be giving the Decker Lecture because of the distinguished position that Major General Charles L. Decker held in the history of the Judge Advocate General's (JAG) Corps and all that he did.[1] He really was a pioneer of the modern military legal system, and particularly of the modern military legal education. And, of course, he was the founder of the specific institution in which we are gathered today.[2]

I notice that Major General Decker graduated from the United States Military Academy at West Point the same year that I was born. So, I guess I am the next generation to his. In any event, I was particularly impressed that Major General Decker had a lasting effect on military law in the United States, as he was one of the drafters of the *Manual for Courts-Martial*, both

---

* This is an edited transcript of a lecture delivered on 6 November 2018 to members of the staff and faculty, distinguished guests, and officers attending the 67th Graduate Course at The Judge Advocate General's Legal Center and School, Charlottesville, Virginia. The lecture is in honor of Major General Charles L. Decker, the founder and first Commandant of The Judge Advocate General's School, U.S. Army, in Charlottesville, Virginia, and the 25th Judge Advocate General of the Army.

† Edwin Meese III served as the seventy-fifth United States Attorney General and is currently the Ronald Reagan Distinguished Fellow Emeritus at the Meese Center for Legal and Judicial Studies.

[1] *See generally* THE ARMY LAWYER: A HISTORY OF THE JUDGE ADVOCATE GENERAL'S CORPS, 1775–1975, at 203–41 (1975).

[2] *Id.* at 217–18.

before and immediately after the Uniform Code of Military Justice was promulgated.[3]

When I entered active duty in 1954 as an artilleryman, I was introduced rather immediately to military law. I was introduced to something that was quite different in many ways than how things are today. Because I had had one year of law school at that time, I got all of the legal assignments in my artillery battalion as an extra duty. For example, I was teaching the Uniform Code of Military Justice, which was then a new entity, to recruits. I also had all kinds of "troop information and education" programs, and I got all of those that had anything to do with law. Also, I was appointed as the trial counsel for special courts-martial. In those days, there were, of course, three types of court-martial. There was the summary court-martial, which was a field-grade officer who was both judge and jury. You also had the general court-martial, which was usually a group of high-ranking officers, where the court was composed of usually five to seven of those officers, and you had a law officer. Those were the titles, and those were the functions.

For the special court-martial, no lawyers were involved whatsoever. The members of the court were usually the commanders of the batteries or companies and other senior officers within the battalion or whatever the organization that had a convening authority happened to be. The trial counsel, who was the prosecutor and also had most of the administrative work compiling the necessary forms and reports and so on, and the defense counsel were not lawyers. They were whomever the battalion commander appointed to have those particular tasks. Terms in those days like "military judge" and "military panel," which are common today, were some decades away. Since I had that responsibility, I had to learn a lot about military law in a very short period of time and to make sure that whatever those reports were at the end of the court-martial when it was over, regardless of the verdict, were properly filled out and utilized.

I do not mention this to give you a history lesson or to wallow in nostalgia but to indicate how far the practice of military law has developed over the last sixty years. As we go back to the beginning of our Republic, the Army JAG Corps has had a long and distinguished history. From Lieutenant Colonel William Tudor's initial tenure starting in 1775, as he served as the legal advisor to George Washington, to your current leader, the Army JAG Corps has been side by side with the combat and support troops in every major conflict since the dawn of our country. Unsurprisingly,

[3] *Id.* at 203–09.

the areas of practice have grown in both scope and sophistication. And they continue to change as the Army itself changes and the circumstances demand.

To a greater extent than ever, judge advocates are now critical advisors to both strategic and tactical decision-making in the field and in the halls of the Pentagon and other command post operations. The breadth of the legal issues that comprise today's Army is truly astounding. As our commanders grapple with day-to-day challenges, such as enforcing good order and discipline, Army judge advocates are there to provide the advice on the latest reforms to the Uniform Code of Military Justice: how to avoid unlawful command influence, how best to investigate and charge a Soldier, and a host of related issues. Those responsibilities have always been the standard fare for military law. Defense counsel, and now the Special Victims' Counsel, work hard to ensure that justice is done and that both the accused and the victims have their rights preserved. And, of course, military judges work to ensure that trials are conducted in a fair and orderly manner, free from unlawful command influence or other taints, whether perceived or actual.

In the meantime, and what really is new to a greater extent, warfighting commanders rely on their staff judge advocates for advice on a range of topics, such as the law of armed conflict, the rules of engagement, and the use of force. They go all the way to detention-related topics today, such as the Geneva Conventions, the interrogation rules, human rights, war crimes, and those other topics that only a few decades ago would have been unheard of. Further, the emerging issues and areas of practice, such as cyber and intelligence law, require the Army JAG Corps to properly train and equip its members with the requisite knowledge to stay ahead on these cutting-edge domains. Finally, at the highest levels of our Government, the combatant commanders, the service chiefs, the Chairman of the Joint Chiefs of Staff, the National Security Council members, and the intelligence community all rely on the legal advice from experienced senior judge advocates from across the services. What you do and the advice you provide on national security issues is critical and enables the national command authority to carry out its constitutional responsibility to protect and defend the United States.

I have heard firsthand of the high quality work that is done by judge advocates, particularly in areas like Iraq and Afghanistan, from my son, who has worked together with some of your leaders there. Particularly, there is one who made his mark for my son, Brigadier General Mark Martins, whom

I believe is known to many of you as one of your top leaders in the field. They worked together, actually, while serving on the staff of General David Petraeus, doing some very important and history-making work in Iraq and Afghanistan.

Today, I would like to discuss with you the topic of what I call "military law in uncertain times." In some ways, uncertainty has always been a constant in a political, governmental, or military environment. But today, the level of "known unknowns," as former Secretary of Defense Donald Rumsfeld once stated, seems higher than we have usually faced. While the Cold War produced many vital concerns, obviously, and a whole series of tough decisions at the highest levels—and I was privileged to watch President Reagan as he was making many of those decisions—at least there was a general common understanding of who the enemy was and what their potentials were, as well as a known history and a relatively predictable set of options for those making the decisions.

By contrast, today, our governmental and military leaders face many novel, difficult situations, which particularly affect legal concepts. To start, our Nation is engaged in the longest continuous armed conflict in history—in the history of the United States, at least—with no clear path to bringing the conflict to a victorious end. Unconventional warfare and the unusual nature of the battlefield—a battlefield virtually without limits—provide complex problems, particularly as they defy the norms and laws of war. Even advances in technology have brought new questions with legal implications. The use of drones, for example, remote targeting, and other things that have advanced the cause of war raise legal and moral issues to be faced by JAG Corps members. Cyberwarfare and electronic surveillance as it is now being practiced invite new litigation and new regulation.

At the same time, the relationships between nations have become more complex and more complicated so that international law and traditional legal principles no longer have an easy application. A good example of this is the increased activity of the International Criminal Court (ICC) and its prosecutorial apparatus, which has created new threats, sometimes even to military personnel potentially in the United States. I will talk a little bit about that later.

To further complicate matters, the Federal courts have adopted new, often inconsistent, approaches to the subject of national defense. This has affected the combat processes as well as the legal jeopardy of our military

personnel. I know that this has had a profound effect on your work and particularly deserves special attention at this school and in these times.

Ignoring historical facts and traditional practice, the Supreme Court has made major changes in recent years, establishing new policy outcomes as guides for decision, which have had serious practical implications for our warfighters. In doing so, the Court has assumed powers that have traditionally been placed within either the executive branch or the legislative branch. All of this has created many new challenges for you, the officials charged with advising our military leaders and providing rules of conduct that will protect our troops from legal jeopardy.

To respond to these challenges requires a sound legal foundation for military lawyers and, for that matter, the rest of the legal and judicial professions. They need this to provide advice and to promulgate legal instruction and directives that can guide commanders and troops working in the field and in garrison. This starts, of course, with a faithful interpretation of our Constitution, which is the bulwark of the rule of law. In an uncertain world, the Supreme Court and the rest of the Federal judiciary must be providing the consistency, the accuracy, and the stability that guides our Nation's legal establishment. Many of the court decisions, particularly some that have been somewhat surprising over the last couple of decades, are directly applicable to you and the exercise of your professional duties. As senior judge advocates, you are on the front lines of our Nation's defense, advising commanders on what the courts have said, or what they might say, in a myriad of circumstances. You do not have the luxury of a lot of time to make decisions, because ever-changing, real-world events on the battlefield require immediate answers, and these answers come from various legal sources. They may come from the Constitution itself, case law, or statutes. Instruction must be placed into directives, regulations, and field manuals to simplify the doctrine contained in those sources. Warfighting decisions are a far cry from those made by civilian judges, including those on appellate courts, who can take all the time they need, safe from harm and thousands of miles away from the battlefield, as they deliberate in the marbled halls of stately courtrooms.

In 1985, when I was at the Department of Justice (DOJ), I was invited to give a keynote address to the House of Delegates of the American Bar Association.[4] I used this exchange to start what I hoped would be a national

[4] Edwin Meese III, Att'y Gen., Dep't of Just., Address to the American Bar Association (July 9, 1985).

dialogue on the proper role of the judiciary in general, and the Supreme Court in particular, concerning the interpretation of the Constitution. The speech that I gave was framed around then-recent decisions of the Supreme Court, which had taken wild directions away from what had been for many decades settled law. The actual cases are not directly relevant to today's talk, but my broader point is that constitutional decisions should follow a jurisprudence of what I called at the time original intention (i.e., how does the Constitution really read?). As I explained at the time, a jurisprudence that is seriously aimed at the explication of original intention would produce defensible principles of law that would not be tainted by ideological predilection.

Fortunately, my speech and others that followed started a national discussion on the topic of originalism and the proper mode of constitutional interpretation. Legal giants such as the late Judge Robert Bork and the late Justice Antonin Scalia drove that dialogue in the academy and in the appellate courts. There are, of course, many others who have contributed to this movement who are too numerous to mention today. I might say that, when I gave that talk to the American Bar Association, it probably would have stayed on the shelves and never been heard from again had Justice Harry Blackmun not taken offense at some of the things I said. A few months later at Georgetown Law School, he gave a talk trying to refute my ideas that the decisions of the Court ought to be based on the Constitution. Once he made that counterpoint and then I gave a refutation to his points, the battle was on. And so, even in law schools today, originalism as a basis for constitutional interpretation is taught, or at least acknowledged, in many courses, depending on the predilections of the professor.

This belief in a jurisprudence of original intention, or as we know it today, original public understanding, reflects what is a deeply rooted commitment to the idea of democracy. That is that government and laws come ultimately through the various processes of government itself, but ultimately from the people and are responsive to the people.

As I said in 1985, our Constitution represents the consent of the governed.[5] The people of the country are the source for the structures and the powers of government. That comes right from the Declaration of Independence, which holds that legitimate governments must respond to, and must be governed by, the acceptance of the governed themselves.

---

[5] *Id.* at 7.

The Constitution, as we know, is the fundamental will of the people, which is why it is fundamental law and why the Constitution, under its own terms, is part of the supreme law of the United States. The other two parts of the supreme law are statues enacted under the Constitution and treaties which are ratified by the Senate.

To allow a court to govern simply by what it views at a particular time as being "fair and decent" rather than what the Constitution actually says is a scheme of government that is no longer "of the people." The essence of democracy would be abandoned if that were the case. The permanent quality of the Constitution also would be weakened. A constitution that is viewed as only what the judges say it is, rather than what it actually says, is no longer a constitution in the true sense of the word. To understand this fully, it is necessary to discuss further the concept of what I call "constitutional fidelity," including adherence to the separation of powers, as the foundation for the Supreme Court jurisprudence. Understanding the genius of our Constitution involves a look at its history.

In 1787, the leaders of what were then the thirteen brand new States were having a hard time accomplishing these functions that were national in scope. They had a hard time defending the country against the armies of other countries—England, France, and others—that were intruding on our borders. They were having a hard time defending our merchant ships at sea from both pirates and the navies of other countries. They had difficulty conducting diplomatic relations abroad, particularly with the European powers.

They were looked down on because international agreements and other diplomatic efforts had to be ratified by all thirteen of the States. They had no real national system for trade and commerce. There was no postal system or national currency. In other words, there were thirteen States, and they could only occasionally achieve unanimity and be able to pass law or take some action which met full agreement. But it was not a successful way to conduct the affairs of a new nation that was entertaining so many different problems.

When they came together in 1787, the leaders faced a dilemma. On the one hand, they wanted to have a central government that would perform the necessary, truly national functions. And it ought to have, as they called it, the energy (i.e., the power) to carry out those functions on a national basis and to have a central body to administer that aspect of government. But, at the same time, they did not want to lose the freedom for which they

had fought so hard during the War of Independence. And so they came up with this solution.

They had studied civilizations going back many centuries and examined other governments around the world. They looked at both the successes and the failures of different structures and legal forms. They determined that the key to protecting freedom was to disperse power as widely as possible. In the Constitution, they separated power vertically and horizontally. They separated it vertically by dividing it between the national Government and the States. Only certain powers enumerated in Section 8 of Article I of the Constitution, as I am sure is familiar to all of you in your legal work, were to be given to the central Government. Unfortunately, many of those "national powers" have, by interpretation, expanded far beyond what the Founders had in mind. But it was the Founders' idea that all other government powers were to be reserved to the States or to the people themselves through their local governments. To further disperse power, the national authorities were divided among three independent and separate branches of the Federal Government: the legislative, the executive, and the judicial.

To make sure that the system worked, the structure and boundaries were further set in the Constitution. The fact that this document was written was a particular achievement, as a written governing charter was unusual in the world at that time. So, the result was a written constitution, a system of checks and balances whereby one branch of Government could be a check on the others, and the limitations of enumerated powers. Furthermore, there was an independent branch of the Government—the judiciary—that had the responsibility of interpreting the Constitution.

To understand constitutional fidelity, you have to begin with the document itself. The Constitution exists as a legal document. We all understand the significance of that fact. A contract, will, warranty, or deed has great legal significance. It must be followed according to what it actually says. Even if a contract may be somewhat ambiguous, the court that is interpreting it has to get back to the original intent of the people who have made the contract initially. In the famous case of *Marbury v. Madison*, John Marshall provided the rationale for judicial review based on the fact that we have a written constitution with a meaning that, as he said, is binding on the judges.[6] He used this phrase: "[I]t is apparent that the framers of the Constitution contemplated that instrument, as a rule for

[6] Marbury v. Madison, 5 U.S. (1 Cranch) 137 (1803).

government of *courts*, as well as of the legislature. Why otherwise does it direct judges to take an oath to support it?"[7]

The Framers chose their words carefully. The language that they chose meant something then and means something today. In some places, it is very specific, such as where it says the Presidents of the United States must be at least thirty-five years of age. In other places, the Constitution expresses principles, such as the right to be free of unreasonable searches and seizures or the guarantees of equal protection under the law and due process of law. The text and the structure of the Constitution is instructive. It contains very little in the way of specific political solutions. Political solutions were left primarily to the elected branches of Government: the Congress and the presidency.

The first three articles set out clearly the scope and limits of three distinct branches of Government, and the powers of each were carefully and specifically enumerated. The Constitution's undergirding premise remains that democratic self-government is based upon the limits of certain constitutional principles, which govern the political process.

A jurisprudence that seeks fidelity to the Constitution is not a jurisprudence of political results. Nor is it one that hinges rulings on popular social theories, moral philosophies, personal notions of human dignity, or preferable policy results. These are matters that elected officials or the people serving under them have the responsibility for deciding. Rather, the Constitution itself is very much involved with process. And it is a jurisprudence that, as I noted, seeks to actually depoliticize the law so that it applies evenly, fairly, and equally to people, regardless of their political disposition.

Originalism has been criticized by some, such as Justice Blackmun, as being old-fashioned or a product of political ideologues who have a cramped view of the Framers' intent. I would disagree with that interpretation or that characterization of the Constitution. The purpose of constitutional limits is to make sure that the Government does not get beyond the control of the people themselves. A jurisprudence that is based on first principles is neither conservative nor liberal. It is neither right nor left. It is a jurisprudence that cares about committing and limiting to each organ of Government the proper ambit of its responsibilities. That may be why Justice Elena Kagan, who had been a law school dean, testified during her Supreme Court

[7] *Id.* 179–80.

confirmation hearing, "[W]e are all originalists."[8] Perhaps it was recognition that it really does make sense to begin one's examination of the meaning of the Constitution by reading the actual words of the text, as is the case of the interpretation of other documents, such as statutes.

With that in mind, let me turn to the role of the judiciary in regard to national security, which is what I am particularly concerned with today. Let us begin with an historical fact. Over the first two centuries of our country, the Supreme Court of the United States has traditionally given great deference to the Commander in Chief on issues of national security. Why was this so? For a variety of reasons, not the least of which is that the Court itself has no particular expertise in national security issues. Most, but not necessarily all, of the justices have not served in the military or the intelligence services. Even today, they do not get routine intelligence briefings like members of the executive branch and select members of Congress. So, they have neither the familiarity with the subject nor the latest information about how matters that are actually transpiring in the world are taking place as far as national defense is concerned.

Nor under the separation of powers principle would it make sense for the Court to have played a major role in the conduct of our Nation's national security. That is because they are the least accountable of the three coequal branches of Government and the least informed as to national security or foreign policy or other geopolitical ramifications of policy decisions. And they are the least equipped to deal with the oftentimes real-time decisions that have to be made in national security.

To sum up this point, I would quote Homeland Security Secretary Mike Chertoff, who gave an important speech at Rutgers University on the ten-year anniversary of 9/11. He entitled it, "The Decline of Judicial Deference on National Security."[9] And he said judges "are not necessarily adapted to weigh the practical exigencies of what happens on the battlefield."[10]

As we know, Article 2 of the Constitution says that the executive power shall be vested in a President of the United States of America. The Founders assigned the President—and the President alone—with the duty

---

[8] *The Nomination of Elena Kagan to be an Associate Justice of the Supreme Court of the United States: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 62 (statement of Elena Kagan, Solic. Gen. of the United States).
[9] Michael Chertoff, *The Decline of Judicial Deference on National Security*, 63 RUTGERS L. REV. 1117 (2011).
[10] *Id.* at 1119.

of being the Commander in Chief of the Army and Navy, and today, they would say the Air Force and the other services. This made eminent sense from a structural standpoint, as well as from an accountability and practical standpoint. That is why the President takes an oath, set in the Constitution, to preserve, protect, and defend the Constitution of the United States.[11] But he is also the leader of the executive branch, and he is the one who decides whether, when, and how to use the military in the defense of our national interests. It is in those rare instances when national security issues ever reached the high court that the justices have traditionally, as Mike Chertoff explained, deferred to the executive branch in those legal issues that came before it. They used the political question doctrine, saying that political questions were matters for the executive or the legislative branch and not for the judiciary. They used this on some similar rationale to avoid getting involved in the conduct of war or other activities of our military forces.

It is worth noting that under our constitutional framework, the President, under Article 2, has independent authority to protect the Nation above and beyond any declaration of war or other statutory authorization for the use of military force. There has been a great deal of debate about this, about what that particular authority involves. But it really is based on the idea that the United States, like all countries, enjoys the inherent right of self-defense. And that is why the President may take such action as he deems necessary to protect the country, including military action. But of course, even that has been somewhat constrained by the War Powers Resolution, in which there are certain reporting requirements and other prescribed relationships between the President and Congress as to how to use that power.[12]

As you all know, there have been many situations in which military troops have been used without any formal declaration of war. You, as judge advocates, are called on to help commanders carry out the President's orders and to make sure that the military's actions are consistent with the laws of war.

There are, of course, certain places where Congress itself has responsibilities and power in relationship to national security. For example, Congress has the power declare war. But in the history of the United States, we have only had eleven instances in which Congress has declared

---

[11] U.S. CONST. art. II, § 1, cl. 8. Officers of the Armed Forces must take an oath to "support and defend the Constitution of the United States against all enemies, foreign and domestic" and to "bear true faith and allegiance to the same." 5 U.S.C. § 3331.
[12] 50 U.S.C. §§ 1549–1550.

war, and that was in regard to five different wars.[13] On the other hand, it has also adopted over forty authorizations for the use of military force. Every authorization is unique in its own depth and scope. And, of course, there have been many other instances where military force has been used at the direction of the President.

In 2001, Congress passed the Authorization for the Use Military Force,[14] which I am sure all of you have probably had a hand in applying in your various responsibilities over the years. The use of that authorization against the Taliban and al Qaeda empowered the President "to use all necessary and appropriate force against those nations, organizations, or persons that he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001."[15] Note that this authorization describes, but does not specifically name, the enemies who can be targeted, contrary to the way in which the declaration of war in December 1941 was rather specific in naming the nations that were to be the target of our military forces.[16]

That authorization, along with another one in 2002 that pertained to Iraq,[17] are the primary statutory authorities that we have been operating on since 9/11 against not only Taliban and al Qaeda, but also persons and forces associated with those organizations, and some even beyond that that had only tenuous connections with those two organizations. The Obama and Trump Administrations, following the original Bush Administration, claim that the 2001 authorization has been used to cover other opponents, including ISIS, as you are well aware.

Now, while the statute normally gives the President the authority to make the determination about which persons or organizations fall within the entities that are covered by the authorization, the courts have played a new and major role in defining the scope, most notably through the cases involved in the Guantanamo detainees' habeas corpus litigation. This has

---

[13] JENNIFER K. ELSEA & MATTHEW C. WEED, CONG. RSCH. SERV., RL31133, DECLARATIONS OF WAR AND AUTHORIZATIONS FOR THE USE OF MILITARY FORCE: HISTORICAL BACKGROUND AND LEGAL IMPLICATIONS 1 (2014).
[14] Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).
[15] *Id.* § 2(a).
[16] *Compare id.*, *with* S.J. Res. 116, 77th Cong. (1941), *and* S.J. Res. 119, 77th Cong. (1941), *and* S.J. Res. 120, 77th Cong. (1941).
[17] Authorization for Use of Military Force Against Iraq Resolution of 2002, Pub. L. No. 107-243, 116 Stat. 1498.

been a whole new step for the court to become involved in national defense issues.

As some have noted, rarely in the history of warfare, and certainly not in U.S. history, have prisoners of war been able to challenge their military detention in court. It would have been unheard of, for example, back in World War II, and I am one of the few in the room here that can remember that rather clearly. For example, it would have been unthinkable for the 400,000 German prisoners of war held in the United States in World War II to be able to challenge their detention in court. And where there were challenges in court to our national security policies, they were often dismissed rather rapidly, as I will discuss in looking at the Supreme Court's landmark World War II-era decisions. One was *Ex parte Quirin*;[18] the other was *Johnson v. Eisentrager*.[19] Both illustrate know the practice of deferring to the president was followed in regard to detainee policy.

In *Ex parte Quirin*, the Supreme Court unanimously determined that the President had the authority to try by military commissions eight German saboteurs and deny them a trial in the Federal courts.[20] You remember that they were the men who came up in a submarine off of Long Island and were to carry out various acts of sabotage and espionage within the United States.

In *Johnson v. Eisentrager*, the Supreme Court was confronted with the claims of twenty-one Germans who were being held at the Landsberg prison, which was an American military facility located in the American zone of occupation in postwar Germany.[21] These men had been captured in China, and an American military commission sitting there had convicted them of war crimes involving collaboration with the Japanese after Germany's surrender. The Germans claimed that their detentions violated the Constitution and international law, as they sought a writ of habeas corpus. The case was ultimately sent to the Supreme Court.

Writing for the Court, Justice Jackson gave the decision in that case, and I might mention that he was very active in this particular field. He had actually taken leave from the Supreme Court to serve as the prosecutor for the Nuremberg trials of leaders of the Nazi and Axis powers for war

---

[18] *Ex parte* Quirin, 317 U.S. 1 (1942).
[19] Johnson v. Eisentrager, 339 U.S. 763 (1950).
[20] *Quirin*, 317 U.S. at 1.
[21] *Eisentrager*, 339 U.S. at 766.

crimes.[22] Having returned to the Court, he wrote that American courts lacked habeas jurisdiction, writing: "We are cited to no instance where a court, in this or any other country where the writ is known, has issued it on behalf of an alien enemy who, at no relevant time and in no stage of his captivity, has been within its territorial jurisdiction."[23]

This was the case in that particular situation. And he went on to write that nothing in the text of the Constitution extends such a right, nor does anything in our statutes. It was through these two cases that the Supreme Court affirmed the President's broad powers to detain enemy combatants for the duration of the conflict when acting pursuant to a declaration of war. The ruling denied the detainees the right to challenge their detention in Federal court. Wartime detention of enemy combatants was not a matter for judicial interference.

But that all changed after 9/11. The Court has become actively involved in wartime detention decisions, and I have no doubt that what they have done has been set forth in the cases that you have studied in your various courses. Through a succession of decisions—*Hamdi v. Rumsfeld*,[24] *Rasul v. Bush*,[25] *Hamdan v. Rumsfeld*,[26] and *Boumediene v. Bush*[27]—the Supreme Court has interpreted that the 2001 authorization and the law of war constrains, rather than supports, the President's power. Professor Jack Goldsmith at Harvard Law School has done a lot of writing on the subject.[28] He served in the DOJ during President George W. Bush's term and handled much of the initial legal actions on the Iraq War. He said that the courts engaged the President during wartime like never before and issued decisions that narrowed presidential power in unprecedented ways. In my opinion, each of the decisions would have come out differently if the Court had exercised its traditional deference to the political branches, interpreted the statutes as they were actually written, and read history as it is, not as the Court wished it were.

---

[22] *See generally* Symposium, *The International Military Tribunal at Nuremberg: Examining Its Legacy Seventy-Five Years Later*, 229 MIL. L. REV. 155 (2021) (discussing Justice Jackson and his role in the International Military Tribunal).
[23] *Eisentrager*, 339 U.S. at 768.
[24] Hamdi v. Rumsfeld, 542 U.S. 507 (2004).
[25] Rasul v. Bush, 542 U.S. 466 (2004).
[26] Hamdan v. Rumsfeld, 548 U.S. 557 (2006).
[27] Boumediene v. Bush, 553 U.S. 723 (2008).
[28] *E.g.*, JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 (2012).

Ray Randolph is a judge of the Court of Appeals for the District of Columbia, which is the appellate court that has been most involved in many of these cases, including the few that have proceeded to the Supreme Court. Judge Randolph once wrote, "[t]o interpret the Constitution in light of history, which is what originalism amounts to, you have to interpret history"[29]—in other words, what has gone before. "How well you perform the task of the historian will determine how accurately you interpret the Constitution."[30] In *Boumediene*, the issue was whether the statute depriving the Federal courts, judges, and justices of jurisdiction over Guantanamo habeas actions violated the suspension clause of the Constitution. "In *Boumediene*, the first question under the Suspension Clause was how far geographically the writ of habeas corpus reached in 1789."[31] In other words, as far as America was concerned, how far back does it go? And Judge Randolph wrote that decision for that court before the case was taken by the Supreme Court. He noted in a 2010 article that "Guantanamo is not now, and never has been, part of this country's sovereign territory."[32] And if Congress recognized that when it defined the United States to exclude Guantanamo Bay in the Detainee Treatment Act of 2005,[33] an analysis of the geographical scope of the writ should turn on the basis of our common law historical understanding.

The important issue was how far the scope of the writ of habeas corpus extends outside of the United States. As a means of deciding what the Constitution said about its use, particularly its use outside the territorial United States, Judge Randolph went all the way back into 1767 and 1773, to lectures at Oxford, England, and looked at what the view of the writ affected in the early days of our country.[34] He wrote that Lord Chief Justice Mansfield, in eighteenth century England, "delivered a lengthy opinion in 1759 stating that the Habeas Corpus Act of 1679, which Blackstone described as the bulwark of English liberties, provided that the writ of habeas corpus did not extend beyond England's sovereign territories."[35] Relying on that concept, along with other historical material, Judge Randolph held that the constitutional writ should not extend to

---

[29] A. Raymond Randolph, *Originalism and History: The Case of* Boumediene v. Bush, 34 HARV. J.L. & PUB. POL'Y 89, 89 (2010).
[30] *Id.*
[31] *Id.* at 91.
[32] *Id.*
[33] Detainee Treatment Act of 2005, Pub. L. No. 109-148, 119 Stat. 2739.
[34] Randolph, *supra* note 29, at 91.
[35] *Id.* (citation omitted).

Guantanamo.[36] The case went from the Court of Appeals in the District of Columbia to the Supreme Court. There were many briefs filed, and none cited a single case, or any contemporary commentary, that indicated that habeas reached beyond the Nation's sovereign territory in 1789. Therefore, it should not reach beyond our sovereign territory today or apply to Guantanamo.

Nevertheless, the Supreme Court ruled that the writ of habeas corpus did extend to detainees in Guantanamo.[37] This opinion caused great concern, even among other justices of the Court. Justice Scalia dissented and, as you may have read various dissents of his, you know he often did not mince words. In this case, he wrote, "Today, for the first time in our Nation's history, the Court confers a constitutional right to habeas corpus on alien enemies detained abroad by our military forces in the course of an ongoing war."[38] He went on to write, "The writ of habeas corpus does not, and never has, run in favor of aliens abroad; the Suspension Clause thus has no application, and the Court's intervention in this military matter is entirely *ultra vires*."[39] Justice Scalia was so enraged by this decision that he said it represented an inflated sense of judicial supremacy. And he predicted dire results, even to the point of saying it would almost certainly cause more Americans to be killed.[40]

This type of judicial decision-making has continued to add to the uncertainty of military combat and the legal aspects surrounding it. What is clear, though, is that the cases that I mentioned before, *Rasul*, *Hamdi*, *Hamdan*, and *Boumediene*, have signaled the Supreme Court's departure from the doctrine of *Eisentrager*, where Justice Jackson himself, in his opinion, approved deference to the executive branch on matters relating to the conduct of war. And he did that because to do otherwise, he said, would hamper the war effort and bring aid and comfort to the enemy.[41]

Nevertheless, these cases control today. And they have created something of a morass of legal questions. These cases seem to ignore some of the practical implications of the use they made of habeas corpus and the way in which they are treating enemy aliens that have been captured. Other judges and scholars have commented on this. For example, Judge Janice

---

[36] Boumediene v. Bush, 476 F.3d 981, 988–94, *rev'd*, 553 U.S. 723 (2008).
[37] *Boumediene*, 553 U.S. at 723.
[38] *Id.* at 826–27 (Scalia, J., dissenting).
[39] *Id.* at 827.
[40] *Id.* at 827–28.
[41] Johnson v. Eisentrager, 339 U.S. 763, 776 (1950).

Rogers Brown, recently retired from the D.C. Court of Appeals, talked about the practical consequences of having habeas corpus review in Guantanamo as it affects the battlefield. What she said is that the process at the tail end—that is, after they have been captured and moved to Guantanamo—is now impacting the front end because when you conduct combat operations, you now have to worry not just about protecting yourself and your buddies, not just about winning the war, winning the battle, accomplishing the mission, but now you have to start collecting evidence.

The habeas corpus idea has also been criticized by others. Another judge at that same court said it seems that the result "gives the military an incentive to avoid custody when possible."[42] Another scholar on this subject, Ben Wittes, recently picked up on that idea. In his book, *Detention and Denial*, he argues that the courts have now created an incentive system to kill rather than to capture.[43] And you can understand in many ways the military results of that kind of incentive. Whatever the result, the conduct of war and dealing with its aftermath will continue to require fresh thinking for those emerging problems that have been coming from the new doctrines that result from these very important decisions.

Let me turn to another serious issue that does face you and your colleagues and will perhaps be even more serious in terms of its potential impact in the future: this whole matter of the ICC. As you know, the United States has never become a party to that court, even though some Presidents thought that might be a good idea.[44] The opposition to the United States becoming involved is concern over the power that is given to the prosecutor and other aspects of the ICC, which are far different from those of courts we have in the United States or in most nations of the free world. And that is why the United States' leadership has wisely avoided becoming entangled in the ICC's web.

The Declaration of Independence tells us that legitimate governments derive their just powers from the consent of the governed. I mentioned that a little while ago in looking back to what the Founders had to say in 1787. What it means is that a legitimate legal system capable of administering criminal law and taking action that deals with the lives and liberty of the people on whom it is imposed have several requirements.

---

[42] Doe v. Mattis, 928 F.3d 1, 42 (D.C. Cir. 2019) (Henderson, J., dissenting).
[43] *See generally* BENJAMIN WITTES, DETENTION AND DENIAL (2010).
[44] *E.g.*, JENNIFER K. ELSEA, CONG. RSCH. SERV., RL31495, U.S. POLICY REGARDING THE INTERNATIONAL CRIMINAL COURT (2006).

First, it must have a specific political body with authority to impact criminal laws. The ICC was established by treaty, to which the United States is not a party.[45] Also, any criminal law system has to have legislation or statutes or some written body of law that defines two things. First of all, jurisdiction and due process—what group of people does it encompass, and what is the process by which facts and law can be combined to make decisions? Second, it has to be able to define the specific conduct that is prohibited. Otherwise, there is no basis on which to judge people's actions or to determine whether those actions violate specific laws. Also, there must be some opportunity for appellate review.

As far as the United States is concerned, these crucial elements are lacking in the ICC. I do not believe there is anything worse for people authorized to use lethal force in combat, as Soldiers do, than having a vigorous and unfettered prosecutor roaming the world looking for work.

How to meet these various challenges that we have talked about today: the way in which the international community works, the new technologies, the way in which the courts have dealt with detainees and through that the prosecution of the war, and the ICC. These are the kinds of challenges that face the legal community, particularly the military legal community, now and in the future. They require careful analysis of existing law and doctrine, as well as a detailed exposition of battlefield situations and the problems that are created by these recent Court decisions and potential exigencies that I have discussed today.

I believe that Congress itself must assume a greater role to exercise its prerogatives under the Constitution, to at least clarify the policies of the United States and determine what the law should be in regard to its implementation. Now, it is true that Congress tried with the Detainee Treatment Act. They have also tried with the Military Commissions Act. But, unfortunately, they have been thwarted by the Court. I think they should continue to exercise legislative responsibility, using what the Court has said as initial guidance, but then fashion corrective legislation, which would solve the problems that I have mentioned. To do that requires considerable strategic thinking to develop imaginative and innovative legal answers to the emerging judicial questions.

---

[45] Rome Statute of the International Criminal Court, 17 July 1998, U.N. Doc. A/CONF.183/9 (2002).

An example of imaginative thinking and action occurred while I was in the DOJ; there was a case in which Congress had acted during the 1980s. A statute for the first time provided extraterritorial jurisdiction for the United States if one of our citizens had been harmed overseas, which gave the military the authority to take action against those who had violated the rights and, in some cases, the lives of American citizens.

There was a particular case where terrorists had taken over a Royal Jordanian aircraft, kidnapped the passengers and crew, including some Americans, and blew up the airplane.[46] Through a series of informants, the Central Intelligence Agency was able to determine one of the major leaders of the particular plot against this aircraft was a man by the name of Fawaz Younis. The Federal Bureau of Investigation (FBI) was able to locate him, but how were they able to arrest him? They were particularly anxious to arrest him under the provisions of this new act so that it could be tested as a legal matter in the United States. It was different from trying to get action by the local governments in the nation where this occurred or to achieve justice overseas. The DOJ wanted to handle this not as a military action but as a civilian arrest and prosecution.

Instead, the military became involved, in cooperation with the legal authorities, but the DOJ and the FBI were the responsive authorities. When they found Younis, he had changed his criminal occupation. He was no longer a terrorist, but was now a drug dealer. They established communication with him through a confidential informant. They told Younis that there was a particular drug kingpin who had a yacht and was interested in making a major drug deal with Fawaz.[47] As a result, they were able to lure him out to this yacht which the FBI had rented. He came on board while the yacht was at sea off the territorial limits of the foreign country.

Younis was now on board the yacht, waiting to meet with the drug kingpin, but the drug kingpin happened to be the Hostage Rescue Team of the FBI. Under this new law, the terrorist leader was arrested by U.S. agents, but they had to make sure they could get the criminal to the United States without invading the sovereignty of any other country or raising some issue of international law that might preclude his proper conviction in the United States. They took him by a Navy boat and put him on an aircraft carrier, where there was a plane waiting for him and his captors. They took him

---

[46] 101 CONG. REC. S4208–09 (daily ed. Mar. 15, 1989) (statement of Sen. Arlen Specter).
[47] *See id.* at S4208.

aboard the plane and flew directly to the United States. It was something like a thirteen-hour flight, and it required aerial refueling en route.

They were able to get Younis from an arrest on the high seas to Washington, D.C., without invading any other country. That precluded any attacks on the ultimate conviction for reasons relating to foreign jurisdiction. Ultimately, the terrorist was prosecuted, convicted, and sentenced to thirty years in prison.[48] He served sixteen of those thirty years and was then deported back to Lebanon. This was a classic example of imaginative and innovative thinking which involved good legal and operational cooperation. In this case, the DOJ, the Central Intelligence Agency, investigative officers, the FBI, and the United States Navy all worked together to achieve a good result.

To conclude, let me just say that military law is in uncertain times. That brings with it unprecedented responsibilities and challenges for both lawyers and operational commanders. I appreciate that at this particularly fine institution, The Judge Advocate General's Legal Center and School, you are doing the necessary research and strategic thinking. You are sharpening the skills that will enable the Army to meet those challenges that I mentioned, with integrity and with expertise. I recognize that your branch insignia, having the sword and the quill, represents the profession of arms and the profession of law with long and noble traditions. I certainly wish you well as you continue to bring honor to both of those professions.

Thank you.

[48] United States v. Yunis, 924 F.3d 1086, 1090 (D.C. Cir. 1991), *aff'g* 681 F. Supp. 891 (D.D.C. 1988), *and* 681 F. Supp. 896 (D.D.C. 1988).