A New Framework for Cyber Operations: Reevaluating Traditional Military Activities and Intelligence Collection in the Digital Age

Major Jeremy Watford*

I. Introduction

For over a generation, and despite the presence of an intelligence officer on every military staff, there has been a stark divide for the purposes of statutory authority and oversight between conventionally military activities (ranging from operational preparation of the environment up to direct application of kinetic effects) and intelligence collection, as it is used as a legal term of art. One action may lay the foundation for the next, and many military operations blend both, but ultimately, each type of action is categorized independently and is often undertaken by different agencies and under different statutory authorities. The statutory basis for such a stark line, bordering on mutual exclusivity, is debatable. But as a cultural concept among the agencies it has remained entrenched over time, despite both intelligence agencies and military services demonstrating the advantages of integration through their operational actions.

Within the cyber domain, this often-blurred line has been increasingly rendered meaningless, at least from an operational perspective, as distinct elements and phases of operations have been compressed. Writing about the recent history of cyber warfare, the author and journalist David Sanger observed that "what makes cyber threats different is that the same implant that is used for surveillance can be repurposed as a weapon."[1] If anything, Mr. Sanger understates the case. During a cyber operation, the same asset, controlled by the same human operator, can readily be utilized for passive intelligence collection, tactical preparation for military operations, or the direct application of force. To the extent that there remains any temporal division between these activities, it may be reduced to a matter of minutes or seconds; in many instances, the activities may occur simultaneously within the same operation.

---

* Major Jeremy Watford is a Judge Advocate in the United States Army and currently serves in the Office of the General Counsel at the National Counterterrorism Center. Major Watford previously earned an LL.M. in National Security Law from the Georgetown University Law Center, an LL.M. in Military Law from The Judge Advocate General's Legal Center and School, a J.D. from Tulane University Law School, and a B.A. from Yale University. The views expressed in this article are those of the author and do not necessarily represent the views of the United States Department of Defense, United States Army, or any other government agency. I would like to thank Professor Todd Huntley, Carl Johnson, and Jonathan Fischbach for their expert advice and instruction that helped shape this article.

1. David Sanger, The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age 164 (2018).

The need to clearly distinguish and categorize these activities is driven largely by two factors—the before-the-fact authorities to execute the action and the after-the-fact oversight and reporting tied to their execution. However, within the cyber domain, these historically distinguishable governmental activities are difficult to actually distinguish. In this light, the conventional and long-standing approach to classifying operations—either as "traditional military activity" (TMA) or "intelligence collection"—is outdated.

The inherent weaknesses of the longstanding framework are by no means a new phenomenon. The traditional siloing of activities in this manner is a function of the conventional understanding of the "Title 10 vs. Title 50 divide" – the idea that military action is exercised within the Title 10 statutory framework, while intelligence collection is exercised, distinctly and separately, under Title 50.[2] This is a concept as widely held as it is inherently misleading. In practice and by statute, Title 50 activities often benefit from the participation and support of military personnel, while on the military side of the "divide" the Secretary of Defense retains authority to collect necessary intelligence under both Title 10 and Title 50.[3] The misunderstanding that Title 10 and Title 50 draw strict, mutually exclusive lines separating military and intelligence activities has long been a source of bureaucratic competition and interagency disputes, and shows little signs of fading even as congressional and executive action have further refined the understanding of what constitutes "military activity" as opposed to "covert action."[4]

The misnomer of a Title 10 vs. Title 50 divide is fully obsolete as applied to modern cyber operations, which blend classically distinct functions through the execution of offensive cyber operations, information operations, and intelligence collection.[5] Congress has provided recent, needed guidance clarifying the military's primacy in the cyber domain by definitively designating cyber operations as a TMA.[6] However, this revised statutory definition still does not fully reckon with the manner in which these operations inevitably overlap and intersect with intelligence collection. The problem is exacerbated as the clear distinction between peacetime and armed conflict is blurred in the current environment of persistent strategic engagement, where peer competition (rather than terrorism)

2. Armed Forces, 10 U.S.C. §§ 101-18506; War and National Defense, 50 U.S.C. §§ 1-4852.

3. Exec. Order No. 12333, 3 C.F.R. 1981 Comp. 200, 46 Fed. Reg. 59941 (Dec. 4, 1981), *reprinted as amended in* 73 Fed. Reg. 45325 (July 30, 2008); Joseph B. Berger III, *Covert Action: Title 10, Title 50, and the Chain of Command*, 67 JOINT FORCES Q. 32, 36 (2012) (discussing the Osama bin Laden raid).

4. 10 U.S.C. § 394(c); *see also* Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SEC. L. & POL'Y 539, 541 (2012) (discussing interagency debates over responsibility for cyber operations); Andru E. Wall, *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action*, 3 HARV. NAT'L SEC. J. 85, 89-90 (2011) (discussing bureaucratic "rice bowls").

5. Laura West, *The Rise of the "Fifth Fight" in Cyberspace: A New Legal Framework and Implications for Great Power Competition*, 229 MIL. L. REV. 273, 276-77 (2021) ("[C]yberspace operations most often require covert action and strongly resemble intelligence activities.").

6. *See* National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1632, 132 Stat. 1636, 2123 (2018).

dominates as the principal national strategy concern.[7] The U.S. now operates in a state of steady, continuous engagement below the threshold of armed conflict, particularly in the related spheres of information and cyber operations.[8] Just as Congress has recognized and codified the Department of Defense's (DoD) authorities in this space, it must be recognized that intelligence collection in the cyber domain requires increased flexibility for the DoD and realistic reevaluation of the existing framework.

More specifically, the operational environment requires a new approach to classifying and evaluating these activities, both in terms of understanding the existing authorities and clarifying the proper oversight. The traditional framework for distinguishing military operational preparation of the environment (OPE) as mutually exclusive and distinct from intelligence collection simply does not map effectively on to operations conducted in the cyber domain. In some cases, there is a substantive difference in the nature of the information collected. Military operations inherently require data collection, often of a more tactical nature. This narrowly-scoped information may not rise to the level of "strategic" or "national" intelligence. However, simply classifying all military information collection as OPE and avoiding the designation of intelligence collection is not an effective solution. It fosters distrust from Congress and perpetuates the fundamental misunderstanding that only civilian agencies (rather than uniformed military forces) are empowered to conduct intelligence collection. The executive and legislative branches can achieve a better and more efficient framework, reflective of both operational and statutory reality, by reaffirming the military's authority for intelligence collection, articulating the still-relevant distinction between OPE and intelligence collection, and acknowledging the reality that rather than falling into one of multiple mutually exclusive categories, modern military operations may often constitute both TMA and intelligence collection simultaneously. In that latter instance, the key reform needed is a revision of the applicable oversight which attaches to intelligence collection when conducted under uniformed military command and control.

This paper proposes a roadmap for how to better frame and view these historically distinct categories in light of the operational reality for modern cyber operations. Part II of this paper provides a brief background of the relevant authorities and oversight for covert action, military operations, and intelligence collection, including a discussion of the Title 10 vs. Title 50 divide. Part III of this paper evaluates the application of these categories to modern cyber operations, particularly in light of U.S. Cyber Command's strategic goals and the "defend forward" philosophy. Part IV of this paper proposes recommendations to better define and

7. West, *supra* note 5, at 274-75.

8. U.S. DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018) (discussing "day-to-day competition" and the intent to "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict"); *see also* Robert Chesney, HOOVER INST., *The Domestic Legal Framework for US Military Cyber Operations*, *in* AEGIS: SECURITY POLICY IN DEPTH, at 1, (Aegis Series Paper No. 2003, 2020).

categorize operations in order to provide necessary maneuver space for military commanders, while also staying true to the existing authorities and maintaining the appropriate role for congressional oversight, most notably by redirecting oversight of military-led intelligence collection from the Congressional Intelligence Committees to the Congressional Armed Services Committees and treating military-led intelligence collection distinct from civilian intelligence activities.

II. BACKGROUND AND RELEVANT HISTORY

A. Early Statutory History

The idea of separate military and intelligence spheres ignores the operational reality and history of the armed services, which have been engaged in intelligence collection activities since their inception, including spies employed directly by General Washington at the earliest battles of the Revolutionary War.[9] The modern separation is traceable to the reorganization of the national security infrastructure in the 1940s. The Central Intelligence Group was created in 1946 by President Harry S. Truman and transformed by Congress the next year into the Central Intelligence Agency (CIA), as part of the National Security Act of 1947.[10] In addition to granting the CIA's intelligence-related authorities, the Act also grants the CIA the authority "to perform such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct."[11] This provision has long been understood to include the authority for "covert action," activities conducted to influence foreign affairs with the role of the United States being neither detected nor publicly acknowledged.[12]

The National Security Act, as amended, is contained in Title 50 of the U.S. code. Title 50 provides authority for a broad range of intelligence activities, notably but not limited to the activities of the CIA, whereas Title 10 exclusively describes operations and authorities within the armed forces.[13] This has led to the short-hand description within the legal and national security communities of "Title 50" and "Title 10" to refer to civilian intelligence authority and military authority respectively. Entrenched over long use, these easy referents helped create and reinforce the notion of wholly distinct spheres of intelligence and military operations. By statute, the DoD actually operates under both Title 10 and Title 50, which (in addition to delineating authorities for the broader intelligence community) provides authorization for the DoD's intelligence activities and preserves

9. DAVID MCCULLOUGH, 1776 27-28 (2006) (discussing U.S. spies employed during the siege of Boston); *Id.* at 223-35 (discussing U.S. spies, including Captain Nathan Hale, employed in New York); *see also* John C. Tramazzo, *An Intelligence Primer for the Second Machine Age*, ARMY L., no. 3, 2019, at 35 (discussing the use of spies and espionage by various military forces throughout history).

10. Chesney, *supra* note 4, at 545.

11. National Security Act of 1947, Pub. L. No. 80-253, § 102(d)(5), 61 Stat. 495, 498 (1947).

12. *See* West, *supra* note 5, at 278-79 (discussing "covert action" as the "fifth function").

13. *See generally* 10 U.S. Code §§ 101-18506; 50 U.S.C. §§ 3001-3243.

those activities "under the direction, authority, and control of the Secretary of Defense."[14] Over time, the evolution of the statutory and oversight framework calcified the divide, although the intelligence community grew its kinetic capacity and the military services continued to develop intelligence assets.

Operationally, the CIA quickly became the primary agency engaged in intelligence collection (particularly human intelligence) below the threshold of armed conflict.[15] However, the CIA's operations were not limited to intelligence collection—psychological operations and foreign information activities broadened the CIA's role in delivering non-kinetic effects to counter the Soviet Union.[16] As covert actions and the capacity for non-military effects became increasingly relevant during the Cold War, the CIA's role in delivering kinetic effects increased. At the same time, the military's independent need for "accurate and timely situation oriented operational and environmental data" remained, and the military often found that reliance on outside support from civilian agencies was insufficient.[17] Tensions between military operations and civilian intelligence, such as the Tehran hostage crisis, drove military development of internal intelligence capabilities.[18] Rather than the CIA displacing the military's organic intelligence collection, the military intelligence apparatus grew in parallel with civilian intelligence—while the CIA simultaneously expanded the scope of its non-intelligence, kinetic operations. However, apart from isolated incidents like Tehran, there was minimal operational conflict between the parallel lines of effort in the decades prior to 9/11.

B. Era of Increased Congressional Oversight

Meanwhile, the latter Cold War years saw new inroads of congressional oversight over both conventional military and intelligence activities. Congress imposed additional military oversight through the 1973 War Powers Resolution (WPR), requiring the executive branch to notify Congress when armed forces are deployed into "hostilities," areas where hostilities are imminent, or into foreign territory "while equipped for combat."[19] The WPR further provided a clock intended to force executive action—military operations must cease after sixty days unless authorized by Congress.[20] However, the WPR did not restrain military operations that fall below the threshold of hostilities, nor did the WPR touch on CIA covert actions that might create kinetic effects abroad.[21] Furthermore,

14. 50 U.S.C. § 401 (1947) (current version at 50 U.S.C. § 3002); *see also* Wall, *supra* note 4, at 91.

15. Chesney, *supra* note 4, at 545.

16. West, *supra* note 5, at 279.

17. Chesney, *supra* note 4, at 546 (discussing Special Operations Forces (SOF) operations during the Tehran hostage crisis in 1979-1980 and the inability of the CIA to provide the necessary tactical intelligence support).

18. *Id.*

19. War Powers Resolution, Pub. L. No. 93-148, § 4(a), 87 Stat. 555, 555-56 (1973 & Supp. 5 1988) (codified at 50 U.S.C. §§ 1541-1548).

20. *Id.* at § 5(b)

21. West, *supra* note 5, at 283.

over time the executive branch has interpreted the threshold for hostilities in a manner that does not necessarily capture all military application or use of force—rather, the determining factors include the limited nature of the mission, military means employed, the risk of U.S. casualties, and the risk of escalation.[22] The WPR put meaningful limitations on the executive ability to deploy "boots on the ground," but left much DoD and CIA activity outside of its scope.

The following year, Congress imposed similar notification and procedural requirements on CIA covert actions through the Hughes-Ryan Amendment, mandating that all such covert actions carry a written finding by the President (determining that the action was "important to the national security") and trigger Congressional notification.[23] Notably, the Hughes-Ryan Amendment did not specifically define "covert action" or even use that phrase, instead imposing its requirements on all CIA activity other than intelligence collection, capturing covert action by implication.[24] The lack of statutory clarity quickly proved troublesome, as the plain language of the statute captured a broad scope of minor activity that was both impractical to route through the procedural requirements of a presidential finding and congressional notification and was below the threshold of what Congress truly intended to impose accountability upon in the wake of the Nixon administration.[25] Congress and the executive eventually compromised to apply a distinction between significant activities requiring a specific finding and regular operations that could be approved and executed on a programmatic basis.[26]

These statutory restrictions on military and covert activity were passed just prior to a similar expansion of intelligence oversight, led by the Church and Pike Committees in Congress. Formed in the wake of multiple public revelations regarding secret government activities and executive branch abuse, the two committees were established in 1975 and led by Senator Frank Church in the Senate and Representative Otis Pike in the House.[27] The Committees were a reflection of public sentiment at the time, critical of CIA activities and perceived overreach during the 1960s and early 1970s, and clashed with the executive branch over declassification, document sharing, and ultimately whether the government

22. Memorandum from Caroline D. Krass, Principal Deputy Assistant Att'y Gen., Off. of Legal Couns., to Eric Holder, Att'y Gen. Authority to Use Military Force in Libya (Apr. 1, 2011), https://perma.cc/P947-U4UR.

23. Foreign Assistance Act of 1974, Pub. L. No. 93-559, § 32, 88 Stat. 1795, 1804 (1804) (codified at 22 U.S.C. § 2422).

24. Chesney, *supra* note 4, at 588 (The Hughes-Ryan Amendment referred to CIA "operations in foreign countries, other than activities intended solely for obtaining necessary intelligence.").

25. *Id*. at 588-89.

26. *Id*. at 590.

27. Stuart Taylor, Jr., *The Big Snoop: Life, Liberty and the Pursuit of Terrorists*, THE BROOKINGS ESSAY (Apr. 29, 2014), https://perma.cc/G46K-THC3 (discussing the impact of the Bay of Pigs and Watergate scandals); Gerald Haines, *Looking for a Rogue Elephant: The Pike Commission and the CIA*, 42 STUDIES IN INTELLIGENCE, no. 5, Winter 1998-1999, at 81 (discussing Seymour Hersh's Dec. 22, 1974, article in the New York Times charging the CIA with domestic operations against anti-war activists).

should be engaged in such secret activities at all.[28] Recognizing that such operations, at a minimum, required clearer accountability, the committees recommended creation of the permanent Committees on Intelligence Activities, which would be granted overall oversight of intelligence collection and covert activities.[29] The recommendations expressed the sentiment of the time that any possible drawbacks of increased procedural requirements and reporting were far outweighed by the "dangers of unchecked secret activities."[30]

The work of the Church and Pike Committees was soon followed by passage of the Foreign Intelligence Surveillance Act (FISA) in 1978, imposing a layer of judicial review if and when intelligence agencies targeted U.S. citizens or permanent resident aliens.[31] Combined with oversight and reporting to the respective congressional intelligence committees, this ensured executive branch intelligence activities were subject to oversight by both the legislature and judiciary.

C. The Intelligence Oversight Framework Solidifies

Executive Order (EO) 12333 provided the capstone to the increased oversight of the 1970s. EO 12333 broadened the Hughes-Ryan requirements, directing "any agency engaged in covert action" to comply with the presidential finding and congressional notification requirements, thereby expanding the scope beyond merely the CIA.[32] The Order also defined the DoD's role in intelligence collection by directing the Secretary of Defense to "[c]ollect (including through clandestine means), analyze, produce, and disseminate information and intelligence [as well as] . . . defense-related intelligence and counterintelligence," undercutting the notion that Title 10 and Title 50 should be read as mutually exclusive with regard to military and civilian intelligence authority and reaffirming the role for the Secretary of Defense in authorizing and supervising intelligence collection relevant to the DoD's mission.[33] However, like the legislative acts preceding it, EO 12333 did not attempt to define the precise contours of covert action. The potential gaps and shortcomings of the resulting oversight requirements were twofold—covert action might inadvertently capture routine, minor activity (the original flaw in Hughes-Ryan), but now might also capture significant actions

28. Haines, *supra* note 27, at 83 (noting that Rep. Pike referred to the CIA as a "rogue elephant," operating without oversight or control); John Prados & Arturo Jimenez-Bacardi, *The CIA's Constitutional Crisis – the Pike Committee's Challenge to Intelligence Business as Usual*, NAT'L SEC. ARCHIVE (Jun. 2, 2017), https://perma.cc/A2M4-59F3.

29. S. REP. No. 94-755, Book 1, at 613 (1976); Haines, *supra* note 27, at 89-90.

30. S. REP. No. 94-755, Book 1, at 613 (1976).

31. Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978); *see also* Taylor Jr., *supra* note 27 (noting that the jurisdictional protections of FISA are rooted in both geography and nationality—intelligence agencies may not intentionally target a "U.S. person" anywhere, or any foreign person inside the U.S., without demonstrating probable cause that the target is working as a foreign agent or on behalf of a terrorist group, and obtaining an appropriate warrant from the Foreign Intelligence Surveillance Court (FISC)).

32. Exec. Order No. 12333, 3 C.F.R. 1981 Comp. 200, 46 Fed. Reg. 59941 (Dec. 4, 1981), *reprinted as amended in* 73 Fed. Reg. 45325 (July 30, 2008).

33. *Id*. at § 1.10; *see also* Wall, *supra* note 4, at 124.

conducted by the military, which historically had not been subject to intelligence committee oversight.[34]

These gaps were finally substantively addressed in the 1991 Intelligence Authorization Act, which defined covert action as any activity (1) conducted by an element of the U.S. government, (2) meant to "influence political, economic, or military conditions abroad," (3) in which the "role of the U.S. Government" must not be intended "to be apparent or acknowledged publicly."[35] On its own, this broad definition would capture most if not all clandestine U.S. activity. The perhaps more meaningful definition lies in the enumerated exceptions, which sought to clearly articulate what was not covert action for the purposes of EO 12333 and Hughes-Ryan. The statute provides that an activity would not constitute covert action if it fell into a list of exceptions including "intelligence collection," TMA, and "routine support" to TMA.[36] The statute itself does not clearly define these exceptions; their parameters must be interpreted from the accompanying committee reports.

The report for the initial draft of the bill defined TMA broadly, encompassing "almost every use of uniformed military forces" and including actions below the threshold of declared war or even imminent hostilities.[37] However, the report clarified that TMA are presumed to be attributable to the U.S. government; when "military elements not identifiable to the United States [are] used to carry out an operation abroad without ever being acknowledged by the United States," such an operation would not constitute TMA.[38] Thus, a merely undetected (clandestine) military operation could fall within the TMA exception, so long as the executive was prepared to accept U.S. government responsibility post-operation. Conversely, a fully unacknowledged military operation would not constitute TMA and thus by exclusion from the exception would be considered a covert action. The Pentagon objected to this proposed definition, concerned that it would capture broad categories of military activity and routine support, including "strategic deception operations, certain peacetime psychological operations, some advance support contingency operations, and certain elements of some counterintelligence operations."[39] Ultimately, President George H.W. Bush vetoed the first version of this bill.[40]

Further negotiation followed, which carved out a larger military exception based upon the institutions and personnel involved. Under the revised definition, a fully unacknowledged military operation would qualify as TMA (and thus not a covert action) if "(1) it was commanded and executed by military personnel, and

34. Chesney, *supra* note 4, at 593.

35. Intelligence Authorization Act for Fiscal Year 1991, Pub. L. No. 102-88, § 602, 105 Stat. 429, 443 (1991), *as amended* (codified at 50 U.S.C. § 413b, transferred to 50 U.S.C. § 3093(e)).

36. *Id*.

37. S. REP. No. 101-358, at 54 (1990).

38. *Id*.

39. H.R. REP. No. 101-725 pt. 1, at 40 (1990).

40. Memorandum of Disapproval for the Intelligence Authorization Act, Fiscal Year 1991, 26 Weekly Comp. Pres. Doc. 1958 (Nov. 30, 1990), https://perma.cc/CCH3-LWXL.

(2) took place in a context in which overt hostilities were either (a) ongoing, or (b) anticipated," meaning approval had been given by the National Command Authorities for the activities and for operational planning.[41] The first prong served to exclude the CIA, thus preserving the focus of covert action oversight on CIA activities and insulating purely military operations. The second prong served to ensure that a similarly high level of executive oversight and decision-making would apply to unacknowledged military activities, in parallel with the presidential finding requirement Hughes-Ryan applied to covert actions. However, the negotiated definition left a perceived oversight gap, insofar as unacknowledged military operations qualifying as TMA were not subject to the same reporting and information-sharing with Congress that apply to covert actions.[42]

Continued revisions to the applicable oversight did little to slow the growth of the CIA's operational reach, as reliance on the CIA for kinetic effects continued as the focus transitioned from the Cold War to counterterrorism. Authorization for lethal covert action can be traced back to the Beirut bombing in 1983 and the resulting National Security Decision Directive (NSDD) 138 which reportedly included language authorizing sabotage and lethal force (although not explicitly assassination).[43] However, authorization for direct lethal action appears to have remained more theoretical than actually utilized through the 1980s and 1990s, and the preference to execute covert activity through local proxy forces remained.[44]

D. Post-9/11 Developments

The CIA's operational posture changed definitively following 9/11.[45] As soon as September 17, 2001, President George W. Bush reportedly signed an order authorizing covert action to "kill or capture" Al-Qaeda terrorists worldwide.[46] Though operational integration between military special forces and the CIA dates back to Vietnam, it reached new heights post-9/11 as some of the earliest ground operations in Afghanistan consisted of Special Operations Forces working with CIA personnel, executing operational plans developed by the CIA.[47] The operational synergy, and attendant confusion over authorities and command, reached a peak in the raid which ultimately killed Osama bin Laden.[48]

Additionally, the CIA developed an exceptional capacity to conduct air campaigns using armed drones in the early 2000s. The CIA conducted its first reported lethal drone strike in November 2002, killing a senior Al-Qaeda leader and five colleagues in a vehicle in Yemen, with the consent of the Yemeni

41. 50 U.S.C. § 413b(e) (2010); *see also* S. REP. No. 102-85, at 46 (1991).
42. Chesney, *supra* note 4, at 600.
43. *Id*. at 549-50.
44. *Id*. at 550-60.
45. Wall, *supra* note 4, at 108.
46. Chesney, *supra* note 4, at 563.
47. Chesney, *supra* note 4, at 578-80; Wall, *supra* note 4, at 109.
48. Berger, *supra* note 3, at 32 (discussing then-CIA Director Leon Panetta's comments about command and control of the operation).

government.[49] Approval for the strike was given by CIA Director George Tenet, and thus, "the CIA and the military found themselves targeting not only the same enemy using the same legal rationale, but also using the same weapons platform."[50] As host-nation consent gave way to "concurrent notification" (meaning host nations were informed of strikes as they were underway or immediately after), CIA drone strikes rapidly increased in frequency from a handful each year during 2005-2008 to 188 such strikes in 2010 alone.[51] As Professor Robert Chesney observed, the CIA's activities in this period functionally resembled "a conventional military conducting an air campaign," increasingly operating like a "globe-spanning combatant command."[52]

Likewise, the military—particularly within the special operations community—experienced a broadened scope of intelligence operations post-9/11. As the military's lead agency for counterterrorism, the Joint Special Operation Command was authorized across a broad area of operations (not limited solely to Iraq and Afghanistan) and the inevitable overlap with the CIA was not limited to kinetic actions.[53] From tracing terrorist financial networks to advising on messaging and strategic information campaigns, the military experienced an increased need and increased authority for intelligence collection, conducting activities in functional areas traditionally in the purview of the CIA.[54]

Those expanded authorities were implemented with the immediate passage of the USA PATRIOT Act (2001), notably Section 215, which eventually provided the foundation for the National Security Agency's (NSA) bulk phone record collection program.[55] However, despite the popular impression of unfettered government access to records, existing authorities were still ill-suited to respond to modern internet and cell phone communications, often requiring the application of a "probable cause" burden (beyond what was Constitutionally required) to intercept foreign communications.[56] Congress granted further authority in 2008 with the FISA Amendments Act, providing for specific targeting of internet communications of "foreign persons located abroad," a provision which quickly provided the basis for the majority of internet content and metadata collection.[57]

---

49. Chesney, *supra* note 4, at 567.

50. *Id*.

51. *Id*. at 568-69.

52. *Id*. at 569, 572.

53. *Id*. at 573, 576.

54. *Id*. at 576.

55. Taylor Jr., *supra* note 27; LAURA DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 24-25 (2016) (discussing the Patriot Act's broadening of pen register and trap-and-trace authority to capture email and internet communications, Sec. 215's expansion of business and personal records obtainable under FISA, and the 2006 Congressional expansion of Section 215 (and favorable FISC interpretation) which enabled bulk phone data collection).

56. The National Security Law Podcast, *Episode 36: NSA General Counsel Glenn Gerstell on Section 702*, at 21:36-22:29 (Sep. 14, 2017) [hereinafter The National Security Law Podcast, *Episode 36*].

57. Taylor Jr., *supra* note 27.

This decade of new authorities represented a significant reversal from the trend of oversight and restriction that dominated the 1970s and post-Cold War era, as the pendulum of public and political sentiment swung firmly in favor of empowering intelligence collection, a sentiment that combined with new technology to drive the greatest expansion of intelligence collection authority in our history. However, to the extent that the passage of time and the attacks of 9/11 had diminished the public suspicion that characterized the Church and Pike years, Edward Snowden's leaks and the subsequent publication of details regarding the NSA's collection—particularly the PRISM program—created a storm of backlash that quickly drew the pendulum back to an atmosphere of distrust.[58]

Fair critiques have been made regarding the volume of information collected, the quality and nature of that information, and the erosion of the divide between foreign intelligence collection and the Constitutional protections applicable to domestic law enforcement matters.[59] However, the wide extent of NSA collection publicized by Snowden differs from earlier scandals in one critical respect. As Joel Brennan, former NSA Inspector General and Senior Counsel, stated: "There has not been a whiff of intelligence abuse for political purposes. [This issue concerns] practices approved by Congress and the federal courts and subject to heavy and effective oversight."[60] Rather than nefarious overreach, the FISA Amendments Act was designed to address the ways in which the original FISA framework had grown unworkable in light of modern internet and cell phone communications.[61]

E. Tensions in the Modern Framework

Bureaucratic territoriality has a major role to play in the modern tension between military and intelligence operations, as agencies compete (in manpower, budget, and authority) over leadership in a particular "lane." The normative view of the CIA as the preeminent agency for U.S. collection of human intelligence and conduct of covert actions creates an atmosphere where military expansion in this arena may be perceived not only as a technical overreach of authority but as diverting critical resources—especially where the DoD's manpower and capacity already far outpace the CIA.[62] That tension is exacerbated by definitions and

58. *See, e.g.*, Alicia Parlapiano, *Comparing Two Secret Surveillance Programs*, N. Y. TIMES (Jun. 7, 2013), https://perma.cc/6HPR-JRX4; Glenn Greenwald, Ewen MacAskill, & Laura Poitras, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, THE GUARDIAN (Jun. 11, 2013), https://perma.cc/2M2Z-YN46; Taylor Jr., *supra* note 27.

59. DONOHUE, *supra* note 55, at 28-29.

60. Taylor Jr., *supra* note 27.

61. The National Security Law Podcast, *Episode 36*, *supra* note 56, at 22:28-24:05. While Section 215 authorities were permitted to lapse by Congress in 2015, Section 702 has remained reauthorized, and it has been lauded by the Department of Justice as "the single most productive authority for counterterrorism and associated collection" and by the National Security Agency as the "single most important operational statute" the Agency utilizes. DONOHUE, *supra* note 55, at 51; The National Security Law Podcast, *Episode 217: Talking with Matt Olsen about DOJ National Security Division*, at 19:50-20:00, (Sep. 14, 2017) [hereinafter The National Security Law Podcast, *Episode 217*].

62. Wall, *supra* note 4, at 89-90.

categorization of activities, reaching back to the 1991 Intelligence Authorization Act, that fail to accurately reflect the operational reality and overlap between different functions.

While the 1991 Act provided some clarity on covert actions and the scope of TMA, the negotiations and contemporary reports do not address definitional separation between intelligence activities, TMA, and routine support to TMA. Functionally, these categories are most reasonably read as intending to exempt both (a) *civilian* intelligence activities, and (b) military operations and related support, from the designator of covert action, leaving the requirements of Hughes-Ryan and EO 12333 to focus primarily on the more operational, non-intelligence activities of the CIA. However, the plain language of the definition suggests that intelligence collection and TMA are wholly distinct and exclusive things.[63]

In reality, collection of military intelligence is plainly historic military activity falling within the traditional scope of military operations, and information gathering could easily constitute routine support. Depending on the nature of information sought and the type of operation, military intelligence collection could independently constitute either TMA or routine support thereof. The 1991 Act does not attempt to clarify those lines, primarily focusing on what should be exempted from covert action requirements.[64] However, this categorization fuels the Title 10 and Title 50 misnomer through its implication that intelligence collection as a whole is something apart from military activity.

This problem is far from theoretical—it implicates which agency should direct an activity, which procedures should apply, and provides a statutory hook by which congressional oversight of intelligence activities may attach.[65] Military information gathering is often classified, within military doctrine, as OPE, and as such is classified as TMA.[66] A report from the House Permanent Select Committee on Intelligence (HPSCI) criticized the frequent use of the designation, stating:

> Clandestine military intelligence-gathering operations, even those legitimately recognized as OPE, carry the same diplomatic and national security risks as

63. 50 U.S.C. § 3093(e)(1)-(2).

64. *Id.*; *see also* S. REP. No. 102-85, at 44-47 (1991).

65. Arguably, placing so much import on this classification is not required by the applicable statutes—if classification as TMA is nothing more than an exception to the requirements for "covert action," it would not necessarily per se avoid any other Congressional notification requirements that attach to intelligence activity. However, this is not how the classification has been interpreted in practice. Chesney, *supra* note 4, at 611.

66. *Operational Preparation of the Environment*, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS (2021). The broad term OPE captures the full spectrum of activities and conduct to prepare and shape the operational environment. The intelligence collection aspect of this function might be more precisely described as "intelligence preparation of the operational environment." *Id.* at *Joint Intelligence Preparation of the Operational Envirnoment*; *see also* JOINT CHIEFS OF STAFF, JOINT PUB. 2-01.3, JOINT INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT (May 21, 2014).

> traditional intelligence-gathering activities. While the purpose of many such operations is to gather intelligence, DOD has shown a propensity to apply the OPE label where the slightest nexus of a theoretical, distant military operation might one day exist. Consequently, these activities often escape the scrutiny of the intelligence committees, and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction.[67]

The report comment carries the implication that the DoD is labeling its activities as OPE with the intent of avoiding intelligence oversight.[68] More likely, the reality is simply that the mutually exclusive definitions governing covert action do not reflect the nature of military operations nor their doctrinal terms.

Military intelligence collection does not exist in a vacuum—it exists to inform and enable military operations. Congress's complaint is not the result of intentional obfuscation by the military but rather a natural result of a statutory scheme that has been interpreted to describe intelligence collection as something entirely exclusive from military activity. The criticism of OPE also ignores the full range of military operations. Joint Publication 3-0 describes "the competition continuum" encompassing an enduring "mixture of cooperation, adversarial competition below armed conflict, and armed conflict."[69] This continuum envisions persistent strategic competition including operations during overt hostilities, peacetime, and "a great deal of space in between."[70] Far from constituting subterfuge or overreach, military OPE is a necessary component of military operations and the congressional criticism results from reliance on an unrealistic statutory scheme interpreted to silo intelligence collection as mutually exclusive from military activity.

Furthermore, it is not at all apparent in terms of statutory authority why military intelligence operations would be outside the jurisdiction of the House and Senate Armed Services Committees, as the HPSCI report claims. To be sure, legislative oversight of intelligence is the product of a much more complex statutory framework, a legacy of the Church and Pike committees, and the respective intelligence committees have expanded their oversight in step with the expansion of intelligence collection authorities post-9/11.[71] Nevertheless, an absence of intelligence committee reporting in this arena is not equal to a lack of congressional oversight—"oversight by the armed services committees is still congressional oversight."[72]

---

67. H. R. REP. No. 111-186, at 49 (2009).

68. *See also* Wall, *supra* note 4, at 101-02 (discussing comments of former CIA General Counsel Jeffrey H. Smith regarding "preparation of the battlefield").

69. JOINT CHIEFS OF STAFF, JOINT PUB. 3-0, JOINT OPERATIONS, at xxv (Jun. 18, 2022).

70. West, *supra* note 5, at 294.

71. Wall, *supra* note 4, at 104, 107-08 (arguing that Congress could clarify much of this issue by reforming oversight of military and civilian intelligence activities to align with (1) control, and (2) funding, eliminating the disconnect whereby congressional intelligence committees seek to exercise oversight of military intelligence but do not control the authorizations or appropriations for those agencies).

72. *Id*. at 109.

Contemporary intelligence oversight is characterized by complexity above all else.[73] The former general counsel of the NSA described it as the "single most regulated entity in the federal government."[74] The popular narrative is that modern technology and expanded authorities have created a "golden age" of surveillance and intelligence collection.[75] In truth, evolving technology cuts both ways, simultaneously making it easier for actors to potentially defeat surveillance and disguise malicious action. While technology has removed many of the logistical challenges associated with long-term surveillance, it also provides tools that frustrate surveillance on multiple fronts.[76] The complexity intrinsic to congressional oversight of intelligence, combined with an "antiquated oversight structure" regarding the perceived military and intelligence divide, "casts a shadow of concern and purported illegitimacy over military operations that resemble activities conducted by intelligence agencies."[77] For over a decade, commenters have recognized that this "stovepiped" view of national security functions is both legally incorrect and "operationally dangerous," as it both misunderstands the relevant authorities as mutually exclusive and fosters interagency conflict and unnecessary bureaucratic competition.[78] The post-9/11 counterterrorism mission, particularly in the way it has divorced operations from clearly defined borders and "battlefields," accelerated the overlapping convergence of the CIA's capacity for kinetic operations and military's capacity and need for intelligence collection.[79] This operational convergence, and attendant competition, reaches a new apex in modern cyber operations and military intelligence activities in the cyber domain.

III. OPERATIONS AND INTELLIGENCE IN THE MODERN CYBER DOMAIN

A. U.S. Cyber Command and Current Cyber Authorities

U.S. Cyber Command (USCYBERCOM) was established on June 23, 2009 as the lead element for U.S. military efforts in cyberspace.[80] The dual-hatted nature

73. David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Law: Introduction*, LAWFARE (May 18, 2013), https://perma.cc/S2XC-BE62; David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Law: Challenges*, LAWFARE (May 19, 2013), https://perma.cc/56RR-E4GX ("[E]ven within the vast U.S. Intelligence Community, relatively few officials have the truly deep knowledge and skills to properly perform a blue-sky review of our surveillance laws.").

74. The National Security Law Podcast, *Episode 36*, *supra* note 56, at [12:35].

75. Peter Swire, *The Golden Age of Surveillance*, SLATE (Jul. 15, 2015), https://perma.cc/F5PG-ZBS4; *see generally* DONOHUE, *supra* note 55 (arguing that the current scope and authority for intelligence collection is excessively broad and insufficiently regulated).

76. David Kris, NATIONAL CONSTITUTION CENTER, *Digital Divergence*, at 1 (WHITE PAPER SERIES: A TWENTY-FIRST CENTURY FRAMEWORK FOR DIGITAL PRIVACY, 2016) (arguing that technology makes it more difficult to geographically locate actors and data within physical space, provides enhanced encryption to communications, and creates challenges via sheer quantity of data the government must filter, process, and analyze for relevant intelligence).

77. Wall, *supra* note 4, at 92.

78. *Id*.

79. *See* Chesney, *supra* note 4, at 578.

80. Memorandum from Sec'y of Def. to Sec'ys of the Mil. Dep'ts et. al., Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Mil. Cyberspace Operations, (Jun. 23, 2009), https://perma.cc/2MSU-AG3F.

of the command, with the Commanding General of USCYBERCOM concurrently assigned as the Director of the NSA, embodies the tension between (a) the operational necessity of integrating military operations and intelligence, and (b) the perceived necessity of maintaining a statutory divide. In his confirmation hearing remarks prior to assuming the role, General Keith Alexander explained that "while there will be, by design, significant synergy between NSA and USCYBERCOM, each organization will have a separate and distinct mission with its own identity, authorities, and oversight mechanisms."[81]

In the immediate years following USCYBERCOM's establishment, cyber attacks along multiple vectors dramatically escalated in both scope and degree of intrusion. China's incursion into Google's networks in 2010 (one among many instances of corporate espionage) and North Korea's retaliatory hack of Sony in 2014 (in response to the unflattering and satirical portrayal of Kim Jong-un in a fictional film) were particularly public examples highlighting the persistent, malicious activity by both state actors and state-sponsored groups.[82] However, the true scope and risk to U.S. interests became most evident following Russia's multi-pronged actions (including both direct hacking and cyber-enabled information operations) during the 2016 presidential election.[83] Russia's efforts laid bare both the vulnerability of domestic democratic structures from foreign cyber operations and the lack of clarity concerning our own cyber operations and legal authorities to respond to foreign action.[84]

The need for clarified agency authorities, rapid response, and a more active defense was clear to Congress as well. The National Defense Authorization Act (NDAA) for Fiscal Year 2019 explicitly provided increased military authority for cyber operations and directed USCYBERCOM to "take appropriate and proportional action in foreign cyberspace . . . to disrupt, defeat, and deter" malicious cyber activities, albeit in specified circumstances and with significant executive oversight.[85] The authorization required an appropriate finding by the National Command Authority and attribution of the malicious cyber activity to Russia, China, North Korea, or Iran.[86] Thus, the 2019 NDAA provided explicit authority (beyond existing Authorizations for the Use of Military Force (AUMF)) for military cyber operations but required high-level executive approval, similar to that

81. *Nominations Before the Senate Armed Services Committee, Second Session, 11[1th] Congress: Hearings Before the Comm. On Armed Services*, 111th Cong. 157 (2010) (statement of LTG. Keith B. Alexander, Nominee to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command).

82. SANGER, *supra* note 1, at 67-74, 100-51; *see also* THE INTERVIEW (Sony Pictures 2014).

83. SANGER, *supra* note 1, at 215-39.

84. *Id*. at 237 ("Only because the gray zone of cyber conflict gave Russians cover did Obama hesitate. By the time he responded, after the election, it was too late.").

85. National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1642(a)(1), 132 Stat. 1632, 2132 (2018).

86. *Id*.

required for covert actions, and limited the battle space in terms of potential targets.[87]

From a constitutional perspective, it is highly questionable whether limited cyber actions even require a specific AUMF or legislative basis, particularly in light of the narrow interpretation of "hostilities" under the War Powers Act.[88] Most cyber activities executed in national defense would fall below the threshold of hostilities, and thus fall squarely within executive constitutional authority without need for additional legislative approval, based on the executive branch factors that informed U.S. military operations in Libya and elsewhere.[89] Viewed through this lens, the 2019 NDAA's cyber provisions are less an actual expansion of executive military authority, in any constitutional sense, and more a clarification of which executive branch would have definitive lead in this new sphere of operations. Whether it is ideal for Congress to referee among the executive departments in this manner is debatable but ultimately not particularly relevant. The practical role of Congress in funding both intelligence and military activities and in defining the scope (and appropriate lead committees) for legislative oversight put Congress in the most effective position to settle the growing interagency conflict.

Congress clarified a second source of uncertainty through Section 1632 of the NDAA, definitively specifying that a "clandestine military activity or operation in cyberspace" constitutes TMA.[90] The conference report for the NDAA lays bare the congressional intent to smooth out interagency debate and clear the lane for DoD leadership in cyberspace: "The conferees see no logical, legal, or practical reason for allowing clandestine traditional military activities in all other operational domains (air, sea, ground, and space) but not in cyberspace."[91] Potentially anticipating some confusion about the use of "clandestine" in the statutory definition, Section 1632 provides that "clandestine military activity or operation" in this context refers both to clandestine is the sense of undetected and in the sense of deniability, assuring that all unacknowledged military cyber activity falls outside the definition of covert action and fully within the scope of TMA.[92] The congressional action in this space goes far toward resolving the interagency debates of the preceding decade, clarifying military leadership in cyberspace and resolving the question of whether secret cyber actions should more properly be

87. *Id*.

88. Chesney, *supra* note 4, at 6-7.

89. Krass, *supra* note 22.

90. 10 U.S.C. § 394(c).

91. H.R. REP. No. 115-874, at 1049 (2018) (Conf. Rep.) (commenting on Section 1632).

92. 10 U.S.C. § 394(f)(1)(A) (2018). This definition is potentially confusing, as the conventional understanding of the terms is that a "clandestine" operation is intended to be undetected at the time of execution but is ultimately attributable to the U.S. if/when discovered, whereas a "covert action" is intended to be both undetected and deniable by the U.S. Much like definitional exemptions of the 1991 Intelligence Authorization Act, which exempted all unacknowledged TMA from the presidential finding and congressional reporting obligations attendant to covert actions, the 2019 NDAA definition provides the same exemption to all unacknowledged military cyber actions.

categorized as TMA or covert action.[93] However, ample uncertainty remains when these operations equally appear to constitute intelligence collection.[94]

B. The Unique Nature of Cyber Operations

In multiple contexts—from conventional kinetic operations to uniquely cyber operations designed to achieve specific cyber effects—the cyber-based mechanisms for collecting information and preparing or executing an operation may appear indistinguishable from traditional intelligence activity. First, cyber operations might simply take the form of information gathering in the cyber domain for the purpose of gathering tactical information in support of conventional action or operational planning. From gathering open-source intelligence in real time via social media, to potential intrusion into closed enemy networks, the proliferation of information (and adversary communications) in cyberspace dictates that it will be a significant source of data relevant to any operation in the physical domains.[95] In this manner, the cyberspace connection may be merely incidental to the underlying operation, using cyber-enabled means and methods to enable conventional operations.

Second, cyberspace is now the primary domain for information operations. Akin to dropping leaflets or utilizing radio broadcasts in the past, the broad range of military influence and information-related activities are increasingly conducted on what is now the dominant information platform. And as Russian activities leading up the 2016 presidential election brought to the fore, information operations in cyberspace are yet another front where persistent engagement goes hand in hand with future strategic peer competition.[96] Although the 2019 NDAA failed to address this element of cyber operations directly, Section 1631 of the 2020 NDAA, "Matters Relating to Military Operations in the Information Environment," authorized the DoD to conduct clandestine operations in the "information environment" to defend against "malicious influence activities carried out against the United States" and clarified that these activities constitute TMA under the same umbrella as other military cyber operations.[97] Much like the 2019 NDAA, the scope of the authorization leaves no doubt as to the congressional intent to empower military activity in this space.[98]

Third, and perhaps most critically, dedicated cyber OPE is intrinsic to the preparation for and conduct of actual offensive cyber operations. In order to execute cyber operations, the military must gain and maintain access to adversary networks, by necessity collecting information and preserving the capacity for an on-

93. West, *supra* note 5, at 309 ("Section 394 . . . open[ed] the floodgates to secret military cyberspace operations.").

94. *Id*. at 276-78 (arguing that statutory changes provided "minor affirmations regarding legal structure . . . [but] created even more questions and concerns").

95. Tramazzo, *supra* note 9, at 36, 41.

96. West, *supra* note 5, at 326.

97. National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, §§ 1631(b)(1), 1631(c), 1631(i)(3), 133 Stat. 1198, 1741-42 (2019) (codified at 10 U.S.C. § 397 n.).

98. West, *supra* note 5, at 328.

demand operation. As former Pentagon Chief of Staff Eric Rosenbach described offensive cyber operations:

> It's very painstaking work. You have the platform which is in some other country in the world, you gain access, you hold persistent access, you try not to be discovered, you have something in there sending information back in some ways . . . When you then want to have a payload, you have to have all those other things.[99]

In some instances, cyber assets "may simply be doing surveillance, but . . . it creates the infrastructures so that if you decide you're going to inject code later and try to actually deliver the payload, you've got a way to go do it."[100] This is OPE in the purest sense, setting the battlefield conditions for potentially immediate execution of an offensive action when directed by the appropriate command authority. Unlike the ability to call in air strikes or fire support on a physical target, "[c]yber operations and campaigns demand operational preparation of the environment" in order to access vulnerabilities, set conditions for the delivery of effects, and "hold targets at risk over time."[101]

The 2019 NDAA specifically defines the authority for clandestine military cyber operations to include various activities below the threshold of armed conflict, including both information operations and "preparation of the environment."[102] However, OPE remains a particular trigger point in the tension between TMA and intelligence collection because, to an outside (e.g., congressional) observer, the actions are fundamentally the same. In his own confirmation hearing for the dual-leadership role of USCYBERCOM and the NSA, General Michael Hayden described the relationship between the two:

> What we're talking about here is what the Department of Defense calls operational preparation of the environment, OPE. It's the ability of Defense to get into an area and know it prior to the conduct of military operations. An awful lot of those activities . . . Are not, in terms of tradecraft or other aspects, recognizably different than collecting human intelligence for a foreign intelligence purpose.[103]

The "legal blood lines[s]" for OPE and foreign intelligence are different, General Hayden continued (referencing Title 10 and Title 50), but "they look

99. The Lawfare Podcast, *Avril Haines, Eric Rosenbach, and David Sanger on U.S. Offensive Cyber Operations,* LAWFARE, at 35:16-35:37 (May 28, 2019).

100. *Id.* at 36:03-36:16.

101. Erica Lonergan, *Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior*, LAWFARE (Mar. 12, 2020) https://perma.cc/6PZD-6RX2.

102. West, *supra* note 5, at 313.

103. *Nomination of General Michael V. Hayden, USAF to be Director of the Central Intelligence Agency: Hearing Before the Select Comm. On Intelligence*, 109th Cong. 116 (2006).

very much the same—different authorities, different purposes, mostly indistinguishable activities."[104]

Despite the protestation of "different purposes," cyber operations tend to dissolve the line bifurcating military and intelligence activities, both technically and conceptually. Technically, the nature of cyber operations requires obtaining and then maintaining access in networks. A cyber implant, once in an enemy network, may passively collect information and report back until later activated to achieve some other effect. Furthermore, the notion of phase lines between different steps of an operation, such as intelligence collection, preparation, and execution, may be dissolved in one contemporaneous action, "converg[ing] the need for collection, analysis exploitation, and attack into one simultaneous operation."[105] The same tools, operated by the same personnel, may simultaneously perform what the statutory framework views as distinct functions. Conceptually, cyber operations may primarily seek to secretly influence conditions abroad, typically the purview of covert action — individual effects of operations may constitute traditional espionage or tactical preparation for a military operation, and, at the extreme, cyber operations may cause dramatic kinetic effects.[106] This presents the risk of allowing the relevant categorization (and thus oversight) to depend simply upon which defining label an operator chooses to apply from among multiple equally accurate options.

Viewed in this light, aligning USCYBERCOM and the NSA under a dual-hatted command makes operational sense.[107] But treating cyber intrusion and data collection as an intelligence collection activity, distinct from offensive cyber operations as a traditional military activity, is a legalistic fiction which ignores the operational reality of "military intelligence collection efforts and operational preparation of the cyber environment by military personnel operating under military command and control."[108] The outdated congressional framework of categorization and attendant oversight has not yet caught up to this reality. Furthermore, the prevalence of cyber activities below the threshold of armed conflict and lack of need for "boots on the ground" suggests that most limited cyber operations will be within executive authority, without running afoul of separation of powers. This creates the perceived gap whereby these activities would go uncaptured by

104. *Id*.

105. West, *supra* note 5, at 296; *see also* Michael Hayden, *Cutting Cyber Command's Umbilical Cord to the NSA*, CIPHER BRIEF (Jul. 17, 2017), https://perma.cc/K2D6-6BAL ("[I]n the cyber domain the technical and operational aspects of defense, espionage, and cyberattack are frankly indistinguishable—they are all the same thing.").

106. West, *supra* note 5, at 296 ("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.").

107. Wall, *supra* note 4, at 122; *see also* West, *supra* note 5, at 274-75 ("[T]he need for shared infrastructure, technical resources, expertise, and even authorities arguably makes this complex structure a necessity . . . at least for now.").

108. Wall, *supra* note 4, at 121.

either the oversight requirements tied to hostilities or the reporting requirements tied to intelligence collection.

C. The Current Operational Environment

As described, cyber operations expose a continuing disconnect between legal oversight and operational reality. That the law would lag behind advancing technology and tactics is not novel—the history of legislation is one of statutes and authorities playing catch up to evolving capabilities. The original FISA is a reflection of the predominant communications infrastructure at the time it was passed, distinguishing between radio communications (primarily domestic) and wire communications (primarily international) for the purposes of warrant requirements.[109] The ubiquity of internet and cellular communications diminished the relevance of radio and wire as useful markers for distinguishing domestic and foreign communications, requiring the passage of the FISA Amendments Act to bring statutory authorities into step with operational reality.[110] However, two additional factors—rooted in the current strategic environment—particularly sharpen the need for reform and ensure that the existing conflict, affecting both interagency competition and congressional oversight, will likely accelerate until it is definitively addressed.

The first factor is USCYBERCOM's strategic objective of persistent engagement. The Command's 2018 strategy document outlines the strategic environment and need to "persistently contest malicious cyber activity in day-to-day competition"[111] This essentially calls for a steady state of existing intrusion into enemy networks—constant low-level operations below the threshold of armed conflict—providing the capacity for quick action. "[D]efending forward," as the strategy describes, includes activities that classically appear to be intelligence collection, such as infiltrating enemy "red space" to counter malicious activity before it can affect our networks.[112] Even the most passive intelligence collection likely requires infiltrating another party's systems or networks, as there is no truly neutral ground (e.g. international waters or outer space) in the cyber domain.[113]

The second factor is the ascendant focus on information operations. As Dmitry Kiselyov, a chief Russian propagandist, stated in 2015, "Information war is now

109. 50 U.S.C. § 1801(f) (2015); United States v. Duggan, 743 F.2d 59, 69-70 (2d. Cir. 1984); *see also* Tyler C. Anderson, Note, *Toward Institutional Reform of Intelligence Surveillance: A Proposal to Amend the Foreign Intelligence Surveillance Act*, 8 HARV. L. & POL'Y REV. 413, 418 (2014).

110. *Id*., at 419.

111. U.S. DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 4 (2018), https://perma.cc/23UK-MYP8.

112. *Id*. (articulating the "defend forward" strategy); JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS, at I-5 (Jun. 8, 2018), https://perma.cc/W5FD-VVWZ (defining "red cyberspace" as "those portions of cyberspace owned or controlled by an adversary or enemy"); *see also* Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," LAWFARE (May 28, 2019) https://perma.cc/2DMZ-V9QH.

113. Lonergan, *supra* note 101.

the main type of war . . . preparing the way for military action."[114] But much like code-based cyber activities, information operations are not limited to instances of active or even imminent armed conflict—indeed, influence and information operations are arguably "most potent" during peacetime.[115] The amplifying effects and relatively low cost of execution tilt the balance of information operations towards cyberspace, particularly with regard to social media.[116] While Russian activity during the 2016 presidential election did include direct cyber intrusions, those activities appear to have been more about testing boundaries and establishing access, rather than attempts to directly affect voting systems or tabulation.[117] The far more influential operations involved the use of social media and disinformation designed to foster political discord and distrust.[118] Russia's success in this space, the cheapness of execution, the lack of international repercussions, and the ubiquity of social media all ensure that this line of attack will escalate in the future.[119] The 2022 National Security Strategy reflects this reality, focusing broadly on strategic competition with major powers and specifically referencing election interference, declaring the intent to respond to any "disruptions to our democratic processes . . . using all appropriate tools of national power."[120]

The "appropriate tools" will inevitably include cyber-enabled operations. But the very flexibility and broad utility of cyber operations again highlights the weakness and inadequacy of traditional statutory definitions. If the cyber asset at issue can simultaneously collect intelligence, cause conventional kinetic effects, or anything in between, categorizing the asset along traditional lines becomes, at best, an academic and legalistic exercise divorced from operational reality.[121] Even if such a categorization is possible after the fact based on how an asset is used in a given instance, accurately categorizing the cyber intrusion or dormant-lying asset prior to execution is virtually impossible. It is akin to being forced, for statutory purposes, to declare whether a Swiss Army Knife is truly a knife, a screwdriver, or a pair of scissors, under a false framework that it must be only one and not the others. The asset may be all of those things, depending upon execution.[122] Insisting otherwise is to be "mired in an obsolete paradigm."[123]

---

114. Peter Pomerantsev, *Inside Putin's Information War*, POLITICO (Jan. 4, 2015), https://perma.cc/8GMM-WY2G *see generally* PETER POMERANTSEV, NOTHING IS TRUE AND EVERYTHING IS POSSIBLE: THE SURREAL HEART OF THE NEW RUSSIA (2014).

115. Laura West, *Beyond Fighting Words: Reconceptualizing Information Warfare and its Legal Barriers*, 8 NAT'L SEC. L. J. 162, 181 (2021). General Valero Gerasimov, Russian Chief of the General Staff, described the modern Russian approach to warfare as one which "merges conventional attacks, terror, economic coercion, propaganda, and . . . cyber." SANGER, *supra* note 1, at 157.

116. *Id*.

117. S. REP. 116-290, at 38-40 (2020).

118. West, *supra* note 115, at 183-85.

119. *Id*. at 186.

120. EXEC. OFF. OF THE PRESIDENT, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 16 (2022), https://perma.cc/JX28-BH3X.

121. Chesney, *supra* note 4, at 580.

122. *Id*. at 607.

123. Wall, *supra* note 4, at 141.

The cyber domain has long been the latest front in the friction created by the operational convergence of military activities and civilian intelligence collection. As early as 2010, reports emerged of turf wars among the executive agencies over who should have lead authority for what were then termed "Computer-Network Operations."[124] The current strategic environment dictates this domain's criticality to national defense—the skirmishes and border-testing that characterize below-the-threshold conflict will continue to play out in cyberspace, and the United States can ill afford the inefficiency of bureaucratic infighting or a lack of clarity regarding authorities and oversight. As Andru Wall observed a decade ago, "Congress's stubborn insistence that military and intelligence activities inhabit separate worlds casts a pall of illegitimacy over interagency support, as well as unconventional and cyber warfare."[125] While the creation of USCYBERCOM and the clarification of cyber operations as TMA have settled a portion of the debate, they fail to fully address the overlap with intelligence collection in the cyber domain.

IV. RECOMMENDATIONS

An appropriate framework governing the intersection of military operations and intelligence collection must reconcile various tensions—it should balance operational needs of the executive with appropriate oversight from the legislature; promote efficient and streamlined interagency cooperation; not undermine civil liberties and public trust; and, ideally, require minimal revision to existing statutory authorities. Much has been written about the potential need for a complete revision of intelligence oversight, driven by its "intolerable complexity," and the risk that a simpler system would inherently be more restrictive.[126] In other words, providing the necessary flexibility and freedom of maneuver while also preserving civil liberties inherently tends towards greater complexity in the regulatory framework. While there may be some merit to that observation, complexity is not a virtue on its own merits. Rather than ensure accountability and public trust, it may just as easily create a structure no one readily understands, undermining faith that the checks and balances of the system are functioning as intended.[127] Furthermore, much of the complexity and resultant uncertainty of our current environment is due to the self-imposed failure to marry statutory interpretation to operational reality in two distinct respects: (1) a misunderstanding of existing military authority to conduct intelligence collection, and (2) misdirected assignment of the congressional oversight that should attach to that collection.

---

124. *See, e.g.*, Kasie Hunt, *Intel Agencies' Internal Turf Wars*, POLITICO (Jan. 20, 2010), https://perma.cc/K8KN-KU63.

125. Wall, *supra* note 4, at 141.

126. David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Law: Conclusion*, LAWFARE (May 21, 2013) https://perma.cc/2B6F-53DA.

127. DONOHUE, *supra* note 55, at 136-37 (2016) (discussing the "problem of redundancy problem"); David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Law: Challenges*, LAWFARE (May 19, 2013), https://perma.cc/32RJ-34CZ.

Regarding these two problems—authority and oversight—the first is something of a red herring. The executive branch possesses the constitutional authority for cyber operations below the threshold of hostilities and the DoD possesses the statutory authority for military intelligence collection in furtherance of its mission and purpose. Contrary understandings are a result of statutory misinterpretation and cultural inertia within the agencies themselves. Consequently, the solution concerns reinterpretation and cultural shift rather than explicit statutory revision or new legislation. The greater problem lies in congressional oversight, concerning what the DoD reports and to whom. The proposed solution similarly requires more in the way of reinterpretation than explicitly new law but is far more challenging in terms of entrenched past practice—reorienting intelligence oversight and reporting such that the intelligence committees retain supervision of civilian intelligence activities, while empowering the armed services committees to provide oversight of activities executed under military command and control.

A. Reaffirming Military Authority to Collect Intelligence

The first issue can be dispensed with the most easily, requiring no additional action through statute or executive order, but rather a shift in the understanding of authorities within the relevant agencies. The recent NDAAs, which explicitly identify information operations and preparation of the environment as elements of military cyber operations (and thus TMA), help bolster this understanding but still rely on potentially misleading doctrinal terms.[128] The root of the DoD's intelligence authority lies not in congressional revisions to the scope of TMA, but rather in Title 50 and EO 12333.[129]

One potential way of avoiding the conflict, as Congress previously observed, is to simply call military-led intelligence collection something else—namely, OPE. Some have argued that this division in nomenclature is entirely appropriate and that Title 50 intelligence efforts under military command and control should simply be classified as OPE rather than intelligence collection.[130] To the contrary, categorizing all military-led information gathering efforts as OPE treats the symptoms of the problem rather than its cause. It is statutorily unnecessary, perceived by those outside the DoD as disingenuous, and is ultimately self-defeating in that it accepts two faulty premises—that the military lacks independent intelligence collection authority, and that such collection should automatically trigger intelligence committee oversight. But neither should the designator of OPE be abandoned where it appropriately applies—it is a term rooted in military doctrine and its scope extends wider than mere intelligence collection. Much of what is obtained to support tactical military operations and ongoing information operations may more properly be regarded as OPE than true intelligence collection.

---

128. 10 U.S.C. § 394(c).

129. 50 U.S.C. § 401 (1947) (current version at 50 U.S.C. § 3002); EXEC. ORDER No. 12333, 3 C. F.R. 1981 Comp. 200, 46 Fed. Reg. 59941 (Dec. 4, 1981), *reprinted as amended in* 73 Fed. Reg. 45325 (July 30, 2008); *see also* Wall, *supra* note 4, at 91.

130. *Id*. at 85.

In applying the labels of OPE and intelligence collection, the relevant executive agencies have historically placed too much emphasis on which agency conducts the collection, which authority (Title 10 or 50) governs, or what form the data takes (with signal data in particular treated as intelligence collection). The more relevant questions are whether the military can collect the needed information without leveraging outside agencies' infrastructure and personnel; whether statutory authority or funding outside of the military is implicated; and, potentially, whether the nature of the intelligence collected implicates the full scope of traditional intelligence oversight. In many instances, military commanders need the latitude to conduct tactical information collection without automatically triggering the involvement of outside civilian personnel and infrastructure, and possess the organic assets and capacity to do so. The critical distinction, in terms of triggering oversight and reporting, should rather be based upon whether the collection is conducted pursuant to military command and control.

Cyber operations will increasingly create simultaneous overlap between military operations and intelligence collection. This does not create a conflict per se because of the DoD's independent authority to function in this area. Likewise, for the purposes of exemptions from the covert action definition, military activities may concurrently qualify for an exemption as both TMA and intelligence collection. Once we move beyond the legalistic fiction attached to the naming conventions, we can turn to the more critical issue of congressional oversight for those intelligence activities conducted with appropriate authority under military command and control.

B. Role of Congressional Oversight

The goal of a revised framework should not be to avoid or diminish congressional oversight of military intelligence collection altogether, but rather to align that oversight where it is best suited. Seeking to entirely minimize oversight is yet another self-defeating proposition—opacity breeds suspicion. The public response to the Snowden revelations, and the resulting congressional hearings, provides a cautionary tale for the risks of conducting clandestine activities without sufficient oversight or reporting—even when within legal bounds.[131] Past litigation before the FISC is equally illustrative. In *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, a telecommunications company challenged NSA collection under the Protect America Act, ultimately far exaggerating the nature of the NSA's activities.[132] The judge characterized the claims as "overblown" and found that the government did not engage in the type of conduct alleged, but not before needless litigation was incurred due to exaggerated fears about what the NSA was actually doing.[133] The lesson is clear—

131. West, *supra* note 5, at 340-41 (arguing that appropriate oversight is critical to "balance the military instrument of power" and preserve public trust).

132. In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008).

133. *Id.*

complete secrecy will often lead outside parties to conclude the worst and fuel fears of government overreach. The obvious need for operational security must be balanced against a sufficient level of transparency and oversight necessary to foster public trust.

Beyond the pragmatic risk of fostering distrust, appropriate oversight is essential to intelligence collection in a democracy, where the authorities exercising that power should be burdened with an accountability mechanism to demonstrate that they are exercising those authorities responsibly.[134] But excessive or convoluted oversight is both administratively burdensome and often less effective.[135] Despite enduring fears of a government panopticon, there is little demonstrable evidence that more substantive oversight is truly needed.[136] Rather than more oversight, or the existing poorly directed oversight, both the executive and legislature would be better served by appropriately routed oversight of military intelligence activity by the respective armed services committees.

Rather than rely upon the standing intelligence committees, the armed services committees are more appropriately suited to this task. Currently, the intelligence committees share jurisdiction over DoD intelligence components with the armed services committees.[137] Much of their jurisdiction, particularly the comparatively broader mandate of the HPSCI, is owing to internal House of Representatives Rules rather than relying on a broader statutory mandate.[138] This includes the HPSCI's self-appointed reach regarding "tactical intelligence" and military information collection activities.[139] Conversely, the House and Senate Armed Services Committees (HASC/SASC) exercise broad jurisdiction over ongoing military operations and exercise their oversight through a multitude of reporting mechanisms. With regard to the Senate, the SASC exercises confirmation and approval authority over the promotions of senior officers and specific nominative command positions.[140] And most critically, the armed services committees control the actual authorization and appropriations process for the military services.[141] With regards to meaningful oversight, the armed services committees are best positioned to actually take responsive action and conduct meaningful supervision within the sphere of military intelligence collection.

The role of the intelligence committees is rooted in the Church and Pike legacy from which they formed, and reflects the expansion of intelligence authorities and oversight post-9/11. But their "oversight is weakened by the bifurcated

134. The National Security Law Podcast*, Episode 217*, *supra* note 61, at 27:30-27:58.

135. DONOHUE, *supra* note 55, at 136-137 (arguing that excessive oversight may result in no one actor taking definitive leadership or responsibility).

136. The National Security Law Podcast, *Episode 36*, *supra* note 56, at 44:08-44:20 (discussing the <1% error rate of compliance incidents regarding NSA collection).

137. Wall, *supra* note 4, at 105.

138. *Id*. at 106; RULES OF THE HOUSE OF REPRESENTATIVES, 111th Cong., Rule X, 11(b)(1)(B), 11(j)(1), at 14, 16 (2009).

139. RULES OF THE HOUSE OF REPRESENTATIVES, 111th Cong., Rule X, 11(b)(1)(B), at 14 (2009).

140. 10 U.S.C. § 601.

141. Wall, *supra* note 4, at 105.

authorization and appropriations process."[142] The 9/11 Commission Report itself recommended restructuring congressional intelligence oversight to better align with the actual authorization and appropriations process.[143] Nor does the role of the intelligence committees, primarily focused on the broader foreign intelligence efforts of the CIA and NSA, align with the specific nature of military intelligence collection, particularly the OPE intrinsic to cyber operations.

The intelligence committees should retain their purview over civilian-led intelligence collection (including the NSA), with revisions to the applicable House and Senate Rules streamlining oversight of intelligence activities conducted under uniformed military command and control to the respective armed services committees. The 1991 Intelligence Authorization Act's definition of covert action was crafted to ensure appropriate accountability of the CIA's non-intelligence related activities—the definitional exemptions were tailored to omit both the CIA's traditional intelligence functions (intelligence collection) and unacknowledged military activity (TMA). The categories were not meant to draw a line in the sand whereby all intelligence collection executed by the military necessarily fell within the purview of the intelligence oversight apparatus. Reforming the jurisdictional scope of the intelligence committees would rectify the OPE versus intelligence collection designations as a trigger for specific congressional oversight; align military intelligence oversight under the committees which more properly control their budget; and conform with the original intent of the 1991 definitional exemptions, wherein intelligence collection was meant to exempt the CIA's traditional mission of intelligence gathering.

V. CONCLUSION

History demonstrates that even as distinct agencies have been assigned primary roles in military operations and intelligence collection, overlap and some degree of convergence are inevitable. Mission creep occurs on both sides. The CIA's scope, and often lead role, in kinetic actions is far beyond what could have been contemplated at its founding. Within the military, the need for operational information drives development of ever-larger capacities for collection and analysis. At the same time, the common understanding of the Title 10 and Title 50 divide has entrenched a focus on intelligence activities as legally separate and apart from military operations, while the legacy of the Church and Pike committees and the progressive expansion of intelligence oversight captured military collection activities within its sweep. Cyber operations have the potential to render the operations and intelligence distinction all but meaningless, particularly if the focus is placed upon what the activity appears to be rather than drawing distinctions based on who is conducting the activity and under what authority.

142. *Id*. at 106-07 ("Congress could end the Title 10-50 debate by simply reforming its oversight of military and intelligence activities and align oversight with the statutory authorities.").

143. NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 420 (2004).

The meaningful division, for the purposes of oversight, should be drawn between intelligence activities conducted by civilian agencies and those conducted under military command and control. Military intelligence collection has been conducted for as long as our military has existed, and the military's authority in this space endures through statute and executive orders. The institutional notion that this sphere is entirely ceded to civilian intelligence agencies should be set aside. Regarding oversight, military-led intelligence collection should be subject to review and supervision by the armed services committees that similarly control the services' authorizations and appropriations. Reorienting tactically-focused military collection away from the intelligence committees would better align both sets of committees with their proper focus and avoid the nomenclature shell game regarding OPE and intelligence collection designations. Reformed oversight would encourage and foster the intelligence-operational integration essential to cyber operations, rather than promote continued uncertainty and interagency competition.