

# CONGRESSIONAL OVERSIGHT OF MODERN WARFARE: HISTORY, PATHOLOGIES, AND PROPOSALS FOR REFORM

OONA A. HATHAWAY, TOBIAS KUEHNE, RANDI MICHEL &  
NICOLE NG\*

## ABSTRACT

*Despite significant developments in the nature of twenty-first century warfare, Congress continues to employ a twentieth century oversight structure. Modern warfare tactics, including cyber operations, drone strikes, and special operations, do not neatly fall into congressional committee jurisdictions. Counterterrorism and cyber operations, which are inherently multi-jurisdictional and highly classified, illustrate the problem. In both contexts, over the past several years Congress has addressed oversight shortcomings by strengthening its reporting requirements, developing relatively robust oversight regimes. But in solving one problem, Congress has created another: deeply entrenched information silos that inhibit the sharing of information about modern warfare across committees. This has real consequences. The Senate Foreign Relations Committee and House Foreign Affairs Committee may have to vote on an authorization for the use of military force against a country without a full understanding of options for covert operations that might achieve*

---

\* Gerard C. and Bernice Latrobe Smith Professor of Law, Yale Law School; J.D. (2021), Yale Law School & Ph.D. (2021), Yale University; J.D. Candidate, Yale Law School (2022); J.D. Candidate, Yale Law School (2022), respectively. We are grateful to Chris Ewell, Annie Himes, Brian Kim, Preston Lim, Ellen Nohle, Alasdair Phillips-Robins, and Mark Stevens for their helpful input from the earliest stages of this project and to Curtis Bradley, Gary Corn, Jean Galbraith, Jamil N. Jaffer, and Heidi Kitrosser for their generous feedback on earlier drafts. We are grateful, as well, to the many current and former U.S. government officials who agreed to speak with us for this Article. We applied for and received an exemption determination from Yale University's Institutional Review Board. The research was deemed exempt under 45 C.F.R. § 46.104(2)(ii) (2018). Congressional Oversight of Cyber Operations, IRB Protocol ID 2000029487 (Determination Date Nov. 30, 2020).

*the same purpose with less risk. The House and Senate Armed Services Committees may be asked to approve a train-and-equip program for a partner force in a nation without knowing that the CIA is already operating essentially the same program. And the House and Senate Intelligence Committees may support a proposed covert operation without understanding the broader foreign policy context, and therefore, the reaction that it might provoke if it were discovered.*

*But there is good news with the bad. If Congress is to blame for this information siloing, Congress is also able to fix it. This Article's discussion of solutions begins with a proposal made by the 9/11 Commission to address information sharing failures—the formation of a super committee to address national security matters. After explaining why this is not the right answer, this Article offers four concrete proposals to remedy the problem. First, Congress should promote inter-committee information sharing by expanding cross-committee membership. Second, Congress should require joint briefings to committees when matters cut across jurisdictional boundaries. Third, Congress should permit members to share classified information with other members under limited, clearly defined circumstances. And fourth, Congress should create a Congressional National Security Council to coordinate cross-cutting national security matters and share mutually relevant information.*

TABLE OF CONTENTS

INTRODUCTION . . . . . 141

I. HISTORY OF CONGRESSIONAL OVERSIGHT OF MILITARY AND INTELLIGENCE ACTIVITIES . . . . . 150

    A. *The Foreign Relations and Foreign Affairs Committees* . . . . . 150

    B. *The Armed Services Committees* . . . . . 154

    C. *The Intelligence Committees* . . . . . 156

II. THE CHALLENGE OF MODERN WARFARE . . . . . 160

    A. *The Post-9/11 Title 10-Title 50 Convergence in Modern Warfare* . . . . . 161

        1. *The Rise of Modern Warfare and Its Oversight Challenges* . . . . . 162

        2. *Congress’s Attempts to Respond to the Challenges of Modern Warfare* . . . . . 167

    B. *Congressional Oversight of Cyber Operations* . . . . . 171

        1. *Early Responses to the Emerging Cyber Domain* . . . . . 171

        2. *Filling Gaps While Entrenching Silos* . . . . . 174

III. THE PATHOLOGY OF MODERN WARFARE OVERSIGHT: INFORMATION SILOING . . . . . 186

    A. *Information Siloing: A Problem of Congress’s Own Making* . . . . . 187

        1. *The Power of the “Must Pass” NDAA* . . . . . 187

        2. *Committee Membership Rules* . . . . . 188

        3. *Classification Restrictions* . . . . . 189

        4. *Inter-Committee Turf Wars* . . . . . 192

    B. *Siloing and Its Implications for Oversight and National Security* . . . . . 194

        1. *Siloing Obstructs Deliberation and Informed Legislating* . . . . . 194

        2. *Siloing Means No Committee Has the Complete Picture* . . . . . 198

        3. *Information Siloing Exacerbates Institutional Jealousies and Impedes Agency Coordination* . . . . . 200

IV. PROPOSALS FOR REFORM . . . . . 201

    A. *Why Not Create a Super Committee?* . . . . . 202

<i>B. Four Proposals for Reform</i> .....	206
1. <i>Expand Cross-Committee Membership</i> .....	208
2. <i>Require Joint Briefings</i> .....	209
3. <i>Modify Classification Procedures</i> .....	210
4. <i>Create a Congressional National Security Council</i> . . .	213
CONCLUSION .....	217

## INTRODUCTION

On October 4, 2017, eleven American Special Forces soldiers traveling with a small Nigerien convoy were ambushed by fighters armed with rocket-propelled grenades, mortars, and heavy machine guns. Four American soldiers—Staff Sergeant Bryan C. Black, Staff Sergeant Jeremiah W. Johnson, Staff Sergeant Dustin M. Wright, and Sergeant LaDavid Johnson—were separated from their unit and left to battle the militants for more than four hours. Their tortuous fight to stay alive was later pieced together after their deaths using video footage from overhead drones and Sergeant Wright’s helmet cam.<sup>1</sup>

Seven months later, on May 10, 2018, the Pentagon produced a 6000-page classified report on the incident but released just an 8-page summary to the public.<sup>2</sup> After the Senate Armed Services Committee (SASC) received a classified briefing from the Pentagon, Senator Tim Kaine accused the military of hiding the true nature of its mission in Niger from Congress: “I have deep questions on whether the military is following instructions and limitations that Congress has laid down about the mission of these troops in Africa.”<sup>3</sup> The legal authorization to conduct a “train-and-equip” mission in Niger was, he argued, “a fig leaf” and the briefing, far from answering questions, raised concerns “about why people are hiding from us what they’re doing.”<sup>4</sup> Republican senator and SASC chairman John

---

1. See Rukmini Callimachi, Helene Cooper, Eric Schmitt, Alan Blinder & Thomas Gibbons-Neff, “An Endless War”: Why 4 U.S. Soldiers Died in a Remote African Desert, N.Y. TIMES (Feb. 20, 2018), <https://www.nytimes.com/interactive/2018/02/17/world/africa/niger-ambush-american-soldiers.html> [<https://perma.cc/SH4G-UDU4>] (noting that Congress had not been properly notified of the mission); Press Release, U.S. Africa Command, U.S. Africa Command Statement on Situation in Niger (Oct. 5, 2017), <https://ne.usembassy.gov/u-s-africa-command-statement-situation-niger/> [<https://perma.cc/Z8LN-GWUL>].

2. *Defense Department Briefing on Niger Ambush Investigation*, C-SPAN (May 10, 2018), <https://www.c-span.org/video/?c4728893/pentagon-report-blames-niger-ambush-series-failures> [<https://perma.cc/DV6X-CYCY>]; U.S. DEP’T OF DEF., OCT 2017 NIGER AMBUSH: SUMMARY OF INVESTIGATION 1 (2018), [https://dod.defense.gov/portals/1/features/2018/0418\\_niger/img/Oct-2017-Niger-Ambush-Summary-of-Investigation.pdf](https://dod.defense.gov/portals/1/features/2018/0418_niger/img/Oct-2017-Niger-Ambush-Summary-of-Investigation.pdf) [<https://perma.cc/H9CH-4NRC>].

3. Joe Gould, *Did Military Hide the Real Mission of the Niger Ambush from Congress?*, DEF. NEWS (May 8, 2018), <https://www.defensenews.com/congress/2018/05/08/did-military-hid-niger-mission-from-congress-key-senator-asks/> [<https://perma.cc/6Y8U-RKEN>].

4. *Id.*

McCain joined in the criticism, stating that he knew “[v]ery little” about the U.S. Special Forces presence in Niger, and “[w]e’re just not getting the information in the timely fashion that we need.”<sup>5</sup> Senator Lindsey Graham, too, complained, “We don’t know exactly where we’re at in the world, militarily, and what we’re doing.”<sup>6</sup>

The members of Congress were right: no one in Congress understood the full extent of U.S. involvement in Niger—or in other countries with similar multi-faceted operations. But this confusion did not result, at least not primarily, from the executive branch hiding what it was doing from Congress. The problem was more pernicious: various elements of the military and covert activities in Niger had been briefed to various congressional committees, but no committee—and no member of Congress—was in a position to put all the pieces together. A former congressional staff member explained:

This was an example of stovepiping within and across committees. From what I could piece together, the DOD [Department of Defense] had sought and Congress approved programming under several different authorities for engaging with the Nigeriens. Some were Title 10 train-and-equip programs, and others were likely special operations authorities for clandestine operations ... Each of them was likely sent up as an individual package to Congress.... [Everything] was notified in pieces. No one was in a position to put those pieces together.<sup>7</sup>

This Article is about the pathologies caused by this “stovepiping”—or what we call “siloeing”—of information about modern U.S. national security operations. The information barriers reflected in

---

5. Karoun Demirjian, *McCain Threatens to Subpoena Trump Aides for Information on Niger Attack That Left 4 U.S. Troops Dead*, WASH. POST (Oct. 19, 2017), [https://www.washingtonpost.com/powerpost/mccain-threatens-to-subpoena-trump-aides-for-information-on-niger-attack-that-left-four-troops-dead/2017/10/19/2106450e-b500-11e7-9e58-e6288544af98\\_story.html](https://www.washingtonpost.com/powerpost/mccain-threatens-to-subpoena-trump-aides-for-information-on-niger-attack-that-left-four-troops-dead/2017/10/19/2106450e-b500-11e7-9e58-e6288544af98_story.html) [<https://perma.cc/J8XY-9GQ7>].

6. Daniella Diaz, *Key Senators Say They Didn't Know the U.S. Had Troops in Niger*, CNN (Oct. 23, 2017), <https://www.cnn.com/2017/10/23/politics/niger-troops-lawmakers/index.html> [<https://perma.cc/M2Z8-2KKQ>].

7. Interview with former Congressional Staff Member #6 (Feb. 19, 2021). The staff member stated that these comments were not based on classified information; these comments were the result of this staff member’s efforts to piece together what happened based on public reports.

the Niger episode are endemic to the entire military, intelligence, and foreign affairs oversight structure as it currently exists. Crucial information about certain activities is often available only to a small cadre of congressional members and staffers. As a result, few members, if any, have access to all the relevant information.<sup>8</sup> This means that members of Congress are sometimes left to make decisions that bear on national security and foreign relations in the absence of essential information. In short, members of Congress lack the full picture of American force capabilities, hindering their ability to fulfill their constitutional role in overseeing the executive branch and helping to protect the country.<sup>9</sup>

When it works as it should, oversight ensures that Congress can serve as an effective check on the executive branch. Congressional oversight is essential to calibrating national decision-making to political and policy concerns; preventing waste, fraud, and abuse; and ensuring government programs respect civil liberties and comply with the law.<sup>10</sup> As outside observers, members of Congress and their staff can identify operational gaps, strategic shortcomings, bureaucratic mission creep, and groupthink. Congressional oversight can also provide democratic legitimacy, especially since national security and foreign policy activities frequently take place outside the public's view.

---

8. *See id.*

9. Article I of the Constitution gives the legislature the power “[t]o declare war,” “raise and support Armies,” “provide and maintain a Navy,” “provide for calling forth the Militia,” and “provide for organizing, arming, and disciplining, the Militia.” U.S. CONST. art. I, § 8. *See generally* Michael J. Glennon, *Strengthening the War Powers Resolution: The Case for Purse-Strings Restrictions*, 60 MINN. L. REV. 1, 6-13 (1975) (arguing that presidential war powers are subordinate to congressional war powers); LAURENCE H. TRIBE, *AMERICAN CONSTITUTIONAL LAW* 231, 234 (2d ed. 1988) (stating that the Constitution empowers Congress to regulate the executive’s war powers); LOUIS HENKIN, *FOREIGN AFFAIRS AND THE CONSTITUTION* 80 (1972) (stating that Congress holds primary war power). Congress also has the constitutional authority, and responsibility, to conduct oversight of the executive branch. *See Watkins v. United States*, 354 U.S. 178, 187 (1957) (“The power of the Congress to conduct investigations is inherent in the legislative process. That power is broad. It encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes.”); *McGrain v. Daugherty*, 273 U.S. 135, 174 (1927) (holding that the Framers intended Congress to have “the power of inquiry—with process to enforce it,” and that the oversight power “is an essential and appropriate auxiliary to the legislative function”).

10. *See, e.g.*, S. SELECT COMM. ON INTEL., COMMITTEE STUDY OF THE CENTRAL INTELLIGENCE AGENCY’S DETENTION AND INTERROGATION PROGRAM, S. REP. NO. 113-288, at xiii-xiv (2014).

Given the importance of oversight, Congress's current information-sharing challenges have real consequences. To take just a few examples: the Senate Foreign Relations Committee (SFRC) and House Foreign Affairs Committee (HFAC) may have to vote on an authorization for use of force without understanding options for covert operations that could achieve a similar purpose with less risk, potentially leading to unnecessary and ill-advised operations. The House Armed Services Committee (HASC) and SASC may be asked to approve a train-and-equip program for a partner force in a nation without knowing that the Central Intelligence Agency (CIA) is already operating essentially the same program—creating the possibility that the overlapping programs might not only waste money, but actually undermine each other. And the House Permanent Select Committee on Intelligence (HPSCI) and Senate Select Committee on Intelligence (SSCI) may support a proposed covert operation without understanding the broader foreign policy context—and the reaction it might cause if discovered.

While Congress's failure to share information across committees may have always been a problem to some degree, it has grown markedly over the last decade with the rise of modern national security operations that do not fit neatly within the committees' jurisdictional boxes. In the wake of 9/11, the rise of light footprint special operations and remotely piloted aircraft (colloquially known as "drones") combined intelligence and military tactics. This led to a blurring of the lines between traditional military oversight, codified under Title 10, and intelligence oversight, codified under Title 50.<sup>11</sup> The convergence of Title 10 and Title 50 has become more pronounced as the share of cross-cutting operations in the U.S. operational structure has grown over the last two decades.<sup>12</sup> The rise in the last decade of cyber operations, which also do not fit

---

11. See Maggie Miller & Laura Kelly, *Congress Struggles on Rules for Cyber Warfare with Iran*, THE HILL (Jan. 12, 2020, 10:30 AM), <https://thehill.com/policy/cybersecurity/477795-congress-struggles-on-rules-for-cyber-warfare-with-iran> [<https://perma.cc/8J4N-C4HF>]; Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SEC. L. & POL'Y 539, 615-16 (2012) (discussing the convergence of Title 10 and Title 50); Andru E. Wall, *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action*, 3 HARV. NAT'L SEC. J. 85, 86-88 (2011).

12. See *infra* Part II.A; see also Chesney, *supra* note 11, at 581-82.

neatly into Congress's existing oversight structure, further complicates the current oversight picture.

As these modern forms of warfare have become increasingly important to U.S. military and intelligence operations, this failure of fit has created more and more glaring problems. To begin with, modern forms of warfare do not easily map onto the War Powers Resolution (WPR) framework governing the use of force. After all, drones, special operations, and cyber operations do not generally involve many "boots on the ground," which some regard as a key trigger of the Resolution's framework.<sup>13</sup> Standing alone, cyber operations in particular have fallen below the threshold for "hostilities" that would trigger the WPR reporting framework.<sup>14</sup> Congress has responded to these challenges in the last few years by iteratively adding reporting requirements for modern warfare operations.<sup>15</sup> But in the process it has left too many members of Congress in the dark about modern warfare operations that are directly relevant to their work.

Drawing on interviews with current and former lawyers and professional staff members in Congress and the executive branch,<sup>16</sup> this Article shows that the siloing problem in modern national security operations has undermined Congress's ability to conduct adequate oversight. This, in turn, threatens to harm U.S. national security. Our focus in this Article is on modern "warfare"—that is, activities involved in war—as well as activities that support them and offer alternatives to them. But the problems we identify are not limited to "warfare"; they affect the entire U.S. national security system. Moreover, in casting a spotlight on the oversight of modern warfare, we aim to illuminate a bigger problem that plagues Congress: it is not structured to efficiently and effectively oversee issues that cross the jurisdictional boundaries of its longstanding committee structure (committees that were in some cases created

---

13. See *infra* notes 135-38 and accompanying text.

14. See *infra* notes 135-38 and accompanying text.

15. See *infra* Part II.A.2.

16. As explained *supra* note \*, we sought and received an exemption from the Yale Human Research Protection Program Institutional Review Board. Unless specifically noted, interviews are anonymous to allow interviewees, many of whom currently work in government, to speak candidly. For any significant assertion, we sought confirmation from multiple sources. All interviews were conducted remotely by Zoom.

over a century ago). This problem is especially pronounced in areas that involve classified information because members of Congress and their staff cannot fill gaps in their knowledge by drawing on publicly available information.

While this Article discusses modern warfare writ large, it places emphasis on cyber operations, which are inherently multi-jurisdictional and therefore a particularly vexing version of the problem. Cyber also represents a growing element of the United States's warfighting capacity.<sup>17</sup> Some observers have argued that Congress does not have sufficient oversight jurisdiction over cyber military operations.<sup>18</sup> To the extent that was once true, recent legislative fixes have expanded Congress's oversight role so that only a few modest gaps remain (assuming executive branch compliance with reporting requirements). Indeed, as a congressional staff member observed, "literally every committee on the Hill has a piece of cyber."<sup>19</sup> But as we will show, the core problem is not lack of oversight—it is that oversight is scattered across committees that fail to share relevant information with other committees that might have a stake in the issue. The recent Cyberspace Solarium Commission criticized congressional oversight for being too dispersed across numerous committees and subcommittees. To address the issue, it recommended the creation of a consolidated committee on cybersecurity.<sup>20</sup> But this proposed solution makes the mistake of viewing cyber in isolation from Congress's other oversight obligations. If adopted, it could solve one problem—the disjointed cyber oversight system—while exacerbating another: the inadequate sharing of information about cyber operations with committees that have related jurisdictions. We propose a different solution that addresses both issues.

---

17. See Tyler K. Lowe, *Mapping the Matrix: Defining the Balance Between Executive Action and Legislative Regulation in the New Battlefield of Cyberspace*, 17 SCHOLAR: ST. MARY'S L. REV. ON RACE & SOC. JUST. 63, 64-66 (2015).

18. See, e.g., *id.* at 92-93; Eric Lorber, Comment, *Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?*, 15 U. PA. J. CONST. L. 961, 1001-02 (2013).

19. Interview with Congressional Staff Member #3 (Oct. 7, 2020).

20. See U.S. CYBERSPACE SOLARIUM COMM'N, REPORT 31, 35-36 (2020), <https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf> [<https://perma.cc/6V5B-Z855>].

The multi-jurisdictional nature of modern warfare is a problem that affects both Congress and the executive branch. But the executive branch has a number of structures that encourage, indeed *require*, collaboration across agencies. Chief among them is the National Security Council (NSC), which creates an extensive process for interagency collaboration, cooperation, and coordination on policy and legal issues.<sup>21</sup> This structure aims to ensure coordination among the executive branch agencies involved in national security matters, regardless of formal agency jurisdiction. Remarkably, there is no corresponding structure on the congressional side. As one interviewee put it:

[T]here have been debates about Congress structuring itself to take a whole of government approach to issues like this. It's hard enough in the executive branch. But they have a number of ways to try to integrate across their functional stovepipes. We still face that problem in Congress. There have been attempts at reform, but none have succeeded.<sup>22</sup>

Simply put, a central problem facing congressional oversight—siloeing—is of *Congress's own making*. It is the result of turf battles and political infighting. That is the bad news. The good news is that a problem created by Congress can be fixed by Congress. While presidential administrations come and go and may bring with them different degrees of compliance with legislative requirements, sustained and improved oversight of modern warfare should begin with structural reform in Congress.<sup>23</sup>

Why, if this problem is of Congress's own making and is within Congress's control to address, has Congress not already acted? At least part of the answer is that most members do not know what they are missing. As one former congressional staffer put it: "There

---

21. See generally RICHARD A. BEST JR., CONG. RSCH. SERV., RL30840, *THE NATIONAL SECURITY COUNCIL: AN ORGANIZATIONAL ASSESSMENT* (2011).

22. Interview with Congressional Staff Member #5 (Jan. 27, 2021).

23. See, e.g., Frank O. Bowman III, *Trump's Defense Against Subpoenas Makes No Legal Sense*, ATLANTIC (Jan. 28, 2020), <https://www.theatlantic.com/ideas/archive/2020/01/trumps-defense-against-subpoenas/605635> [<https://perma.cc/EM4X-VPHR>]; Burgess Everett & Josh Dawsey, *White House Orders Agencies to Ignore Democrats' Oversight Requests*, POLITICO (June 2, 2017, 5:11 AM), <https://www.politico.com/story/2017/06/02/federal-agencies-oversight-requests-democrats-white-house-239034> [<https://perma.cc/VP9U-L9WS>].

aren't many members worked up about this issue, because they don't have a full view of the problem."<sup>24</sup> He continued: "They may get the information they think they should be getting. But they don't know the information they aren't getting access to. The same is true of the staff level. They do not know what they do not know."<sup>25</sup> Moreover, those who do have most of the information—especially members of the so-called Gang of Eight,<sup>26</sup> which includes congressional leadership—are not always interested in sharing.<sup>27</sup>

This Article proceeds in four parts. Part I shows how Congress has constructed three distinct oversight channels for military and intelligence operations: the foreign relations and foreign affairs committees to oversee country missions, use of force, and war powers; the armed services committees to oversee the Department of Defense (DOD) and its Title 10 operations; and, most recently, the intelligence committees to provide oversight of the intelligence community and its operations, most of which are conducted under Title 50. Part II then turns to the challenges posed by the rise of modern forms of warfare. Since 9/11, military and intelligence capabilities have increasingly converged.<sup>28</sup> As the DOD developed its own intelligence tools and clandestine programs,<sup>29</sup> and the CIA acquired new lethal capabilities (most notably, drones),<sup>30</sup> the separate oversight regimes became both more incoherent and spotty. Recognizing the emerging oversight gaps, Congress began in 2011 to pass statutes specific to special forces, lethal strikes, and cyber

---

24. Interview with former Congressional Staff Member #6, *supra* note 7.

25. *Id.*

26. The "Gang of Eight" includes the House and Senate minority and majority leaders as well as the HPSCI and SSCI chairs and ranking members. See 50 U.S.C. § 3093(c)(2).

27. The same is generally true of the intelligence committees, which are particularly protective of their access. Interview with Jamil N. Jaffer, former Chief Counsel to the Senate Foreign Relations Committee (under Chairman Bob Corker (R-TN)) and former Senior Counsel to the House Permanent Select Committee on Intelligence (under Chairman Mike Rogers (R-MI)) (Jan. 21, 2021) ("The intelligence committees don't regularly provide TS/SCI [Top Secret/Sensitive Compartmented Information] access to noncommittee members because they jealously protect access to such sensitive materials.").

28. See Corri Zoli, *The Changing Role of Law in Security Governance: Post-9/11 "Gray Zones" and Strategic Impacts*, 67 SYRACUSE L. REV. 613, 626 (2017).

29. See Eric Schmitt & Thom Shanker, *Threats and Responses: A C.I.A. Rival; Pentagon Sets Up Intelligence Unit*, N.Y. TIMES (Oct. 24, 2002), <https://www.nytimes.com/2002/10/24/world/threats-and-responses-a-cia-rival-pentagon-sets-up-intelligence-unit.html> [<https://perma.cc/7Q35-FRCY>].

30. See Chesney, *supra* note 11, at 566 (discussing the CIA's "kinetic turn").

operations,<sup>31</sup> granting larger oversight roles to HASC and SASC.<sup>32</sup> But while this approach filled oversight gaps and clarified ambiguities, it also reinforced and entrenched existing divisions in committee jurisdictions.<sup>33</sup> Part III discusses the key pathology that this system has produced: information siloing. We argue that information siloing has prevented relevant committees from receiving critical national security information, impeding their ability to conduct informed lawmaking—a key function of congressional oversight. Moreover, we show that Congress, not the executive, has created these oversight challenges through committee infighting and turf protection. Part IV turns to solutions, offering proposals for ensuring members of Congress and the committees are fully informed so that Congress can more effectively carry out its law-making duties and serve as a meaningful check on the executive.

---

31. When this Article speaks of cyber, it discusses cyber operations specific to modern warfare. Cybersecurity, such as working with private companies to secure domestic networks, is beyond the scope of this Article. For more information on congressional oversight of cybersecurity, see Carrie Cordero & David Thaw, *Rebooting Congressional Cybersecurity Oversight*, CTR. NEW AM. SEC. (Jan. 30, 2020), <https://www.cnas.org/publications/reports/rebooting-congressional-cybersecurity-oversight> [<https://perma.cc/C672-VVWA>]. Likewise, foreign election interference through misinformation and disinformation campaigns on social media is also beyond our scope. See, e.g., Mark Scott, *Russia Is Back, Wilier than Ever—And It's Not Alone*, POLITICO (Sept. 14, 2020, 4:30 AM), <https://www.politico.com/news/2020/09/14/russia-cyber-attacks-election-413757> [<https://perma.cc/WW29-62DC>].

32. See Kelsey D. Atherton, *Trump Inherited the Drone War but Ditched Accountability*, FOREIGNPOL'Y (May 22, 2020, 12:57 PM), <https://foreignpolicy.com/2020/05/22/obama-drones-trump-killings-count> [<https://perma.cc/R7K9-EQ6M>].

33. This Article focuses on the armed services, intelligence, and foreign relations committees because they have the most significant oversight roles over modern warfare operations. See Cordero & Thaw, *supra* note 31. Of course, other agencies and their respective oversight committees may sometimes be involved in modern warfare operations. For example, the Department of Justice's controversial legal analyses of the CIA's enhanced interrogation techniques created oversight equities for the judiciary committees. See HUM. RTS. WATCH, NO MORE EXCUSES: A ROADMAP TO JUSTICE FOR CIA TORTURE 2 (2015), <https://www.hrw.org/report/2015/12/01/no-more-excuses/roadmap-justice-cia-torture> [<https://perma.cc/Z36M-T5J2>]. See generally S. REP. NO. 113-288 (2014). The judiciary committees also engage with cybersecurity oversight in the context of surveillance, cybercrime enforcement, and data privacy. See Cordero & Thaw, *supra* note 31. The homeland security committees may play a related oversight role. See *id.* For example, the Department of Homeland Security is responsible for securing civilian cyber infrastructure and coordinating cybersecurity efforts with the private sector. See *id.*

## I. HISTORY OF CONGRESSIONAL OVERSIGHT OF MILITARY AND INTELLIGENCE ACTIVITIES

This Part examines the congressional committees that are primarily involved in overseeing military and intelligence operations. First, the Senate Foreign Relations Committee (SFRC) and House Foreign Affairs Committee (HFAC) oversee foreign missions, authorizations of the use of military force, and war powers reporting.<sup>34</sup> Second, the House Armed Services Committee (HASC) and Senate Armed Services Committee (SASC) oversee the DOD and “traditional military activities” conducted under Title 10.<sup>35</sup> And third, the House Permanent Select Committee on Intelligence (HPSCI) and Senate Select Committee on Intelligence (SSCI) handle intelligence oversight—operations that generally take place under the Title 50 authority of the CIA and other intelligence agencies and programs (including, at times, DOD intelligence programs).<sup>36</sup> As we will see in the next Part, these committee structures may have worked well for traditional warfare, but they have proven a poor fit in the era of modern warfare.

### A. *The Foreign Relations and Foreign Affairs Committees*

Foreign affairs have been subject to informal, ad hoc oversight by the House and Senate since the Founding.<sup>37</sup> As the young Republic’s diplomatic business grew steadily over the first few decades, both chambers soon created standing committees to oversee it: SFRC

---

34. See *Guide to House Records: Chapter 10*, NAT’L ARCHIVES, ¶ 10.1, <https://www.archives.gov/legislative/guide/house/chapter-10.html#CmtForeignAffairs1810> [<https://perma.cc/6X8Q-C4LU>] [hereinafter *HFAC Background*]; S. COMM. ON FOREIGN RELS., BACKGROUND INFORMATION ON THE COMMITTEE ON FOREIGN RELATIONS OF THE U.S. SENATE, S. DOC. NO. 105-28, at 4 (2000) [hereinafter *SFRC BACKGROUND*].

35. See Wall, *supra* note 11, at 102-03, 122; STANDING RULES OF THE SENATE RULE XXV(c)(1), S. DOC. NO. 113-18, at 20 (2013), <https://www.govinfo.gov/content/pkg/CDOC-113sdoc18/pdf/CDOC-113sdoc18.pdf> [<https://perma.cc/JD9S-J7KB>] [hereinafter *SENATE RULES*].

36. See Wall, *supra* note 11, at 101-05.

37. See *HFAC Background*, *supra* note 34, ¶ 10.1; *SFRC BACKGROUND*, *supra* note 34, at 4.

was established in 1816<sup>38</sup> and HFAC followed in 1822.<sup>39</sup> Although the precise jurisdictions of the foreign relations committees have shifted over the centuries, they have always been responsible for oversight of relations with other nations.<sup>40</sup> In recent years, this has translated into jurisdiction over the State Department, including U.S. embassies abroad, and the U.S. Agency for International Development (USAID).<sup>41</sup>

The committees have traditionally overseen decisions to declare war, authorize traditional military interventions, and shape relations with foreign nations.<sup>42</sup> That jurisdiction has been deeply connected to the War Powers Resolution (WPR)<sup>43</sup> since its passage in 1973.<sup>44</sup> Enacted in response to concerns that the executive branch had abused its war powers in Southeast Asia,<sup>45</sup> the WPR requires the President to notify and consult Congress regarding the introduction of armed forces into hostilities;<sup>46</sup> provide periodic updates to Congress throughout the duration of involvement in hostilities;<sup>47</sup> and withdraw armed forces from hostilities after sixty days unless

38. SFRC BACKGROUND, *supra* note 34, at 4.

39. HFAC Background, *supra* note 34, at 10.2.

40. See SFRC BACKGROUND, *supra* note 34, at 4-6. Unless specifically noted otherwise, “foreign relations committees” refers collectively to both the House Foreign Affairs Committee and Senate Foreign Relations Committee.

41. H. COMM. ON RULES, 116TH CONG., RULES ADOPTED BY THE COMMITTEES OF THE HOUSE OF REPRESENTATIVES OF THE UNITED STATES 143 (Comm. Print 2019) [hereinafter HFAC RULES]; S. COMM. ON FOREIGN RELS., 117TH CONG., RULES OF THE COMMITTEE ON FOREIGN RELATIONS 1 (Comm. Print 2021) [hereinafter SFRC RULES].

42. See HFAC RULES, *supra* note 41, at 143; SFRC RULES, *supra* note 41, at 1.

43. See 50 U.S.C. § 1541.

44. See War Powers Resolution, Pub. L. No. 93-148, 87 Stat. 555 (1973).

45. See Edwin B. Firmage, *The War Power of Congress and Revision of the War Powers Resolution*, 17 J. CONTEMP. L. 237, 248-49 (1991); see also LOUIS FISHER, *PRESIDENTIAL WAR POWER* 128 (1995).

46. 50 U.S.C. § 1542 (“The President in every possible instance shall consult with Congress before introducing United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and after every such introduction shall consult regularly with the Congress until United States Armed Forces are no longer engaged in hostilities or have been removed from such situations.”); *Id.* § 1543(a)(3)(A)-(C) (“In the absence of a declaration of war” the President must submit a report within forty-eight hours detailing “the circumstances necessitating the introduction of United States Armed Forces; the constitutional and legislative authority under which such introduction took place; and the estimated scope and duration of the hostilities or involvement.”).

47. *Id.* § 1543(c) (requiring the President to update Congress on the status, scope, and duration of hostilities no less than once every six months).

otherwise authorized by Congress.<sup>48</sup> WPR oversight, along with congressional decisions to authorize the use of military force (AUMF), fall under the jurisdiction of the foreign relations committees.<sup>49</sup> The WPR's rigorous restraint provisions came under attack almost immediately after it was passed. Presidents since Nixon have questioned the constitutionality of the WPR,<sup>50</sup> although they have generally complied with its reporting requirements by filing reports "consistent with the War Powers Resolution."<sup>51</sup> The WPR's ambiguity and interpretive flexibility—especially regarding the term "hostilities"—has limited its scope and practical effect.<sup>52</sup> The WPR does not define what constitutes "hostilities," and no legislation or court decisions have offered more specificity.<sup>53</sup> Even though

48. The sixty-day limit can be extended for thirty days by the President if he certifies that "unavoidable military necessity respecting the safety of United States Armed Forces" requires their continued use in the course of bringing about their removal. 50 U.S.C. § 1544(b).

49. See Press Release, U.S. Senate Comm. on Foreign Rels., Senators Propose Legislation to Update Authorities Used to Fight Terror Abroad (Apr. 16, 2018), <https://www.foreign.senate.gov/press/chair/release/senators-propose-legislation-to-update-authorities-used-to-fight-terror-abroad> [<https://perma.cc/XW3U-7YWS>].

50. President Nixon vetoed the WPR, which Congress overrode. Veto of War Powers Resolution, 9 WEEKLY COMP. PRES. DOC. 1285 (Oct. 24, 1973). Nixon believed that the legislation was unconstitutional because it would undermine the President's war powers. *Id.* at 1286. In particular, he took issue with the sixty-day withdrawal provision and the provision permitting Congress to mandate withdrawal of forces through concurrent (now joint) resolution. See *id.*; see also Louis Fisher & David Gray Adler, *The War Powers Resolution: Time to Say Goodbye*, 113 POL. SCI. Q. 1, 2-6 (1998) (providing an account of the legislative history of the WPR); Robert F. Turner, *The War Powers Resolution at 40: Still an Unconstitutional, Unnecessary, and Unwise Fraud that Contributed Directly to the 9/11 Attacks*, 45 CASE W. RESV. J. INT'L L. 109, 127 (2012) (arguing that the WPR is unconstitutional). For counterarguments, see, for example, Stephen L. Carter, *The Constitutionality of the War Powers Resolution*, 70 VA. L. REV. 101, 101 (1984).

51. CONG. RSCH. SERV., R42699, THE WAR POWERS RESOLUTION: CONCEPTS AND PRACTICE 23-25 (2019). From 1975 through March 2017, Presidents submitted 168 reports pursuant to the WPR. *Id.*; see also TESS BRIDGEMAN, REISS CTR. ON L. & SEC., WAR POWERS RESOLUTION REPORTING: PRESIDENTIAL PRACTICE AND THE USE OF ARMED FORCES ABROAD, 1973-2019, 16-17 (2020), <https://warpowers.lawandsecurity.org/wpr-reporting-1973-2019.pdf> [<https://perma.cc/9FX5-ARWL>].

52. For a discussion of a much larger pattern in which Congress is generally hesitant to exercise strong oversight over military operations, instead focusing on oversight over administrative military matters such as acquisitions, training, and equipping, see Mark Patrick Nevitt, *The Operational and Administrative Militaries*, 53 GA. L. REV. 905, 938-49 (2019).

53. Trevor W. Morrison, "Hostilities," 1 J.L. (1 PUB. L. MISC.) 233, 236 (2011); Oona A. Hathaway, *How to Revive Congress' War Powers*, in POLICY ROUNDTABLE: THE WAR POWERS RESOLUTION, TEX. NAT'L SEC. REV. 41, 43-50 (Nov. 14, 2019), <https://tnsr.org/roundtable/policy-roundtable-the-war-powers-resolution/> [<https://perma.cc/MRQ9-FLSX>].

the WPR's legislative history suggests that Congress intended "hostilities" to be a broad term,<sup>54</sup> Presidents have interpreted it narrowly to avoid reporting requirements and triggering its withdrawal provisions.<sup>55</sup> In 2011, for example, as the WPR sixty-day termination date for U.S. military operations in Libya neared, the Obama administration concluded that U.S. military operations did not constitute "hostilities" within the meaning of the WPR even though the United States had already conducted an extensive bombing campaign.<sup>56</sup> The Trump administration subsequently adopted a similar position on "limited" hostilities in Syria.<sup>57</sup> And in Yemen, President Trump argued that U.S. military operations in support of the Saudi-led coalition did not amount to "hostilities," as U.S. troops served only in a noncombat support role, despite a resolution supported by both houses of Congress specifically labeling the operations "hostilities."<sup>58</sup>

The executive branch's narrow interpretation of the WPR has cabined its scope and thus limited the foreign relations committees' ability to exercise their intended oversight role. As one

---

54. H.R. REP. NO. 93-287, at 7 (1973) ("[H]ostilities was substituted for the phrase *armed conflict* during the subcommittee drafting process because it was considered to be somewhat broader in scope.... [H]ostilities also encompasses a state of confrontation in which no shots have been fired but where there is a clear and present danger of armed conflict.").

55. See Curtis A. Bradley & Jean Galbraith, *Presidential War Powers as an Interactive Dynamic: International Law, Domestic Law, and Practice-Based Legal Change*, 91 N.Y.U. L. REV. 689, 697 (2016); Chesney, *supra* note 11, at 612; Hathaway, *supra* note 53, at 43-50.

56. *Libya and War Powers: Hearing Before the S. Comm. on Foreign Rels.*, 112th Cong. 7-9 (2011) (statement of Harold Koh, Legal Adviser, U.S. Department of State); UNITED STATES ACTIVITIES IN LIBYA 25 (2011), in Letter from Joseph E. Macmanus, Acting Assistant Sec'y, Legis. Affs., Dep't of State & Elizabeth L. King, Assistant Sec'y, Legis. Affs., Dep't of Def., to Hon. John A. Boehner, Speaker, House of Representatives (June 15, 2011), <https://fas.org/man/eprint/wh-libya.pdf> [<https://perma.cc/L5E2-DE9A>].

57. See Memorandum Opinion from Steven A. Engel, Off. of Legal Couns., to the Couns. to the President, April 2018 Airstrikes Against Syrian Chemical-Weapons Facilities (May 31, 2018).

58. S.J. Res. 7, 116th Cong. (2019). The resolution was vetoed by President Trump. Message to the Senate Returning Without Approval Legislation Regarding the Removal of United States Armed Forces from Hostilities in Yemen, 2019 DAILY COMP. PRES. DOC. 1 (Apr. 16, 2019). Congress has repeatedly considered revisions to the War Powers Resolution to address the problems outlined in this Section, but it has yet to implement any changes. See, e.g., *Reclaiming Congressional War Powers: Hearing Before the H. Comm. on Foreign Affs.*, 117th Cong. (2021), <https://foreignaffairs.house.gov/2021/3/reclaiming-congressional-war-powers> [<https://perma.cc/8YX8-QUQ9>]; War Powers Reform Resolution, S.J. Res. 60, 116th Cong. (2019); *War Powers Reform Resolution*, H.J. Res. 83, 116th Cong. (2020); War Powers Reform Act, H.R. 383, 113th Cong. (2013).

congressional staffer explained, “The foreign relations committees never managed to have the hook they should have had through the War Powers Resolution. They used it as a rhetorical cudgel rather than as an operative means to have a seat at the decision-making table.”<sup>59</sup> As modern warfare tactics have increasingly fallen outside the WPR’s scope,<sup>60</sup> the foreign relations committees have been increasingly sidelined. As discussed in the next two Sections, much of that oversight authority has instead gone to the armed services and intelligence committees.

### *B. The Armed Services Committees*

In the mid-twentieth century, in response to the immense growth in U.S. power and influence abroad, Congress took its first major steps to institute a statutory framework for authorizing and overseeing U.S. military activities.<sup>61</sup> After World War II, Congress enacted the National Security Act of 1947 to restructure the country’s foreign policy, military, and intelligence establishments.<sup>62</sup> Among many other significant structural changes, the National Security Act reorganized military authorities under a single Department of Defense (DOD), with its organization and functions primarily codified in Title 10 of the U.S. Code.<sup>63</sup>

Created in 1946, SASC and HASC were charged with “exercis[ing] continuous watchfulness” over this new Defense Department and its programs and authorizations.<sup>64</sup> SASC exercises jurisdiction over the DOD and the service branches and “stud[ies] and review[s], on a comprehensive basis, matters relating to the common defense

---

59. Interview with Congressional Staff Member #4 (Jan. 19, 2021).

60. See *infra* Part II.A; see also Eric Talbot Jensen, *Future War and the War Powers Resolution*, 29 EMORY INT’L L. REV. 499, 535-43 (2015).

61. See Chesney, *supra* note 11, at 584-86.

62. National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495.

63. 10 U.S.C. §§ 101-18505. See generally OFF. OF SEC’Y OF DEF., THE DEPARTMENT OF DEFENSE: DOCUMENTS ON ESTABLISHMENT AND ORGANIZATION 1944-1978, v-vi, 35-36, 40-45 (1978), <https://history.defense.gov/Portals/70/Documents/other/DODDocsEstandOrg1944-1978.pdf> [<https://perma.cc/52KD-R723>].

64. Legislative Reorganization Act of 1946, Pub. L. No. 79-601, § 136, 60 Stat. 812, 832 (1946); see James M. Lindsay, *Congressional Oversight of the Department of Defense: Reconsidering the Conventional Wisdom*, 17 ARMED FORCES & SOC’Y 7, 9 (1990).

policy of the United States.”<sup>65</sup> HASC exercises similar jurisdiction over the DOD and the “[c]ommon defense generally,”<sup>66</sup> including the “laws, programs, and agencies under ... [T]itle 10.”<sup>67</sup>

DOD activities conducted under Title 10 are subject to the armed services committees’ oversight.<sup>68</sup> Title 10 also contains more than 300 reporting requirements to be made to Congress, ranging from spending breakdowns to readiness assessments and strategy reports.<sup>69</sup> Congressional oversight thus spans fiscal and budgetary issues, management and performance, and policy and strategy.<sup>70</sup> One significant means by which the armed services committees exercise oversight is the annual National Defense Authorization Act (NDAA), which “establishes or continues defense programs, policies, projects, or activities at DOD and other federal agencies, and provides guidance on how the appropriated funds are to be used in carrying out those authorized activities.”<sup>71</sup>

As we shall see in Part II, the armed services committees have been able to use their control over the “must pass” NDAA to fill oversight gaps and in the process have granted themselves greater oversight roles over potentially multi-jurisdictional modern

65. SENATE RULES, *supra* note 35, R. XXV(c)(1)-(2) at 19-20.

66. RULES OF THE HOUSE OF REPRESENTATIVES, 116TH CONG., R. X(1)(c)(2)-(8), 6 (2019), <https://rules.house.gov/sites/democrats.rules.house.gov/files/documents/116-House-Rules-Clerk.pdf> [<https://perma.cc/RA4M-NJ2Y>] [hereinafter HOUSE RULES].

67. H. COMM. ON ARMED SERVS., 116TH CONG., OVERSIGHT PLAN FOR THE 116TH CONGRESS 3, [https://armedservices.house.gov/\\_cache/files/b/2/b236a61e-6d45-40cd-9ad8-bc99b83dfa3b/AE1FC7A607C9432146B32AF84E99181B.hasc-oversight-plan-for-the-116th-congress.pdf](https://armedservices.house.gov/_cache/files/b/2/b236a61e-6d45-40cd-9ad8-bc99b83dfa3b/AE1FC7A607C9432146B32AF84E99181B.hasc-oversight-plan-for-the-116th-congress.pdf) [<https://perma.cc/ZH82-9TD7>].

68. Wall, *supra* note 11, at 102. Nine Department of Defense elements—the Defense Intelligence Agency (DIA); the National Security Agency (NSA); the National Geospatial-Intelligence Agency (NGA); the National Reconnaissance Office (NRO); and intelligence elements of the Army, Navy, Marine Corps, Air Force, and Space Force—are conducted under Title 50 authority and therefore fall under the intelligence committees’ jurisdiction.

69. CLERK OF THE U.S. HOUSE OF REPRESENTATIVES, REPORTS TO BE MADE TO CONGRESS, H.R. DOC. NO. 116-85, at 1, 28, 31, 83 (2020).

70. *See, e.g.*, Lindsay Wise, *House Passes War Powers Resolution Limiting President’s Ability to Strike Iran*, WALL ST. J. (Mar. 11, 2020, 6:15 PM), <https://www.wsj.com/articles/house-passes-war-powers-resolution-limiting-presidents-ability-to-strike-iran-11583961365> [<https://perma.cc/CP5F-BM23>]. In addition to formal oversight channels through hearings, members of Congress also exercise oversight through unofficial communications about defense programs and consideration of legislation. *See id.*

71. BRENDAN W. MCGARRY & VALERIE HEITSHUSEN, CONG. RSCH. SERV., IF10516, DEFENSE PRIMER: NAVIGATING THE NDAA (2021). *See infra* Part II for more analysis on the role of the NDAA.

warfare.<sup>72</sup> Their control over this annual authorization process also ensures that the DOD is generally quite responsive to the armed services committees' requests—and even protective of the committees' jurisdiction. In fact, the DOD sometimes resists efforts by other committees to request briefings on matters that fall within HASC and SASC jurisdictions, both to guard against multiple overseers and to avoid angering the committees to which they are most directly beholden. As one former staff member put it, "DOD's position is that we talk to HASC and HAC-D [House Appropriations Defense Subcommittee] because that's who controls our money and conducts our oversight."<sup>73</sup> Thus, as the foreign relations committees' influence over modern warfare has declined over the course of the last several decades, the armed services committees' influence has continued to grow.

### C. The Intelligence Committees

The intelligence committees are the most recent additions to the national security committee system.<sup>74</sup> They were initially created in response to a crisis: in late 1974, the *New York Times* published a series of devastating articles that exposed covert CIA operations infiltrating antiwar student protests,<sup>75</sup> interfering with foreign elections,<sup>76</sup> and opening mail from the Soviet Union to the United

---

72. See *infra* Part II.

73. Interview with Jamil N. Jaffer, *supra* note 27.

74. See Loch K. Johnson, *The Contemporary Presidency: Presidents, Lawmakers, and Spies: Intelligence Accountability in the United States*, 34 *PRESIDENTIAL STUD. Q.* 828, 830 (2004).

75. 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), <https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html> [<https://perma.cc/Y5HG-U9SH>] [hereinafter Hersh, *C.I.A. Operation*]; Seymour M. Hersh, *Helms Disavows "Illegal" Spying by the C.I.A. in U.S.*, *N.Y. TIMES* (Dec. 25, 1974), <https://www.nytimes.com/1974/12/25/archives/helms-disavows-illegal-spying-by-the-cia-in-us-special-to-the-new.html> [<https://perma.cc/KS6Q-RCC7>]; Seymour M. Hersh, *Underground for the C.I.A. in New York: An Ex-Agent Tells of Spying on Students*, *N.Y. TIMES* (Dec. 29, 1974), <https://www.nytimes.com/1974/12/29/archives/underground-for-the-cia-in-new-york-an-ex-agent-tells-of-spying-on.html> [<https://perma.cc/B5ZS-J9KK>].

76. Seymour M. Hersh, *C.I.A. Said to Have Asked Funds for Chile Rightists in '75*, *N.Y. TIMES* (Oct. 21, 1974), <https://www.nytimes.com/1974/10/21/archives/cia-said-to-have-asked-funds-for-chile-rightists-in-73-a.html> [<https://perma.cc/M4LU-UWF9>].

States.<sup>77</sup> Revelations mounted that the CIA was domestically spying on U.S. citizens in violation of its own charter.<sup>78</sup> In December 1974, Congress passed the Hughes-Ryan Amendment,<sup>79</sup> which “provided the first statutory basis for notification to Congress and congressional oversight of covert action operations.”<sup>80</sup> In early 1975, the Senate created the Church Committee,<sup>81</sup> and the House created the Pike Committee to investigate intelligence abuses.<sup>82</sup> Their reports cemented the view that there needed to be permanent oversight over the intelligence agencies, prompting Congress to establish HPSCI and SSCI.<sup>83</sup>

At the time, members of Congress raised concerns about overlapping jurisdictions and information sharing across committees. Senator Walter Mondale explained that “[r]esponsibility and authority are fragmented in several committees,” making it “impossible to look at intelligence as a whole.”<sup>84</sup> The select committees were designed to include at least one member from each of the appropriations, armed services, judiciary, and foreign affairs/relations

77. Hersh, *C.I.A. Operation*, *supra* note 75.

78. The CIA’s domestic spying activities were aptly abbreviated as “Operation CHAOS.” See BRIAN FREEMANTLE, *CIA 122* (1983). For an overview of Operation CHAOS, see *Halkin v. Helms*, 690 F.2d 977, 982-84 (D.C. Cir. 1982).

79. Hughes-Ryan Amendment, Pub. L. No. 93-559, 88 Stat. 1804 (1974) (codified as amended at 50 U.S.C. § 3093) (prohibiting the use of appropriated funds for covert actions unless the President makes a “finding” that those actions are important to U.S. national security interests and has submitted that finding to the six appropriate committees, which were later expanded to the “Gang of Eight,” in a timely manner); see *infra* note 100 and accompanying text.

80. MICHAEL E. DEVINE, CONG. RSCH. SERV., R45175, *COVERT ACTION AND CLANDESTINE ACTIVITIES OF THE INTELLIGENCE COMMUNITY: SELECTED DEFINITIONS IN BRIEF 2* (2019).

81. Thomas Young, *40 Years Ago, Church Committee Investigated Americans Spying on Americans*, BROOKINGS INST. (May 6, 2015), <https://www.brookings.edu/blog/brookings-now/2015/05/06/40-years-ago-church-committee-investigated-americans-spying-on-americans> [<https://perma.cc/M7YD-8NT7>].

82. *The White House, the CIA and the Pike Committee, 1975*, NAT’L SEC. ARCHIVE (June 2, 2017), <https://nsarchive.gwu.edu/briefing-book/intelligence/2017-06-02/white-house-cia-pike-committee-1975> [<https://perma.cc/23S2-QR6R>].

83. See Johnson, *supra* note 74, at 830. SSCI’s mission is to “make continuing studies of [U.S.] intelligence activities and programs, ... to submit to the Senate appropriate proposals for legislation[,] report to the Senate concerning such intelligence activities, [and] assure that such activities are in conformity with the [law].” *About the Committee*, S. SELECT COMM. ON INTEL., <https://www.intelligence.senate.gov/about> [<https://perma.cc/YGA8-DSR6>].

84. FREDERICK M. KAISER, CONG. RSCH. SERV., *LEGISLATIVE HISTORY OF THE SENATE SELECT COMMITTEE ON INTELLIGENCE 45* (1978).

committees.<sup>85</sup> Senator Abraham Ribicoff explained the importance of dual memberships: "If this is going to work at all, there has to be comity between the standing committees, the select committee, and the executive branch of our Government .... It is inconceivable to me that any intelligence matter would be kept back from the parent committee."<sup>86</sup> He continued, "It is definitely our intention if there is any matter of importance involving any other committee ... [that] the Intelligence Committee [will inform] the Committees on Armed Services, Foreign Relations, Judiciary, or Appropriations."<sup>87</sup> However, Senator William Taft predicted that individual senators with dual memberships would face challenges transmitting appropriate information "in light of the provision which requires the full Select Committee on Intelligence to develop regulations governing such transmittal."<sup>88</sup>

Congressional debates especially focused on ensuring that the armed services and intelligence committees "make every effort to assist and facilitate the work of the two committees."<sup>89</sup> To promote information sharing, the two committees issued a Memorandum of Understanding, agreeing that

[w]here there are questions of joint concern between the Senate Select Committee on Intelligence and the Senate Armed Services Committee, they will be promptly made a matter of consultation and resolution between the Chairmen of the two Committees, the full Committees, and the Chiefs of Staffs of both Committees as may be appropriate.<sup>90</sup>

Today, congressional rules also mandate that the chair and ranking member of SASC serve as ex-officio SSCI members.<sup>91</sup>

---

85. *About the Committee*, *supra* note 83. The SSCI includes one majority and one minority member from each of these committees. *Id.* House rules require at least one member from each committee to serve on the HPSCI. HOUSE RULES, *supra* note 66, R. X(11)(a)(1) at 14.

86. 122 CONG. REC. 14,171 (1976) (statement of Sen. Abraham Ribicoff).

87. *Id.* at 14,172.

88. KAISER, *supra* note 84, at 49.

89. *Id.* at 60 (quoting *Memorandum of Understanding Between the Chairman of the Senate Select Committee on Intelligence and the Chairman of the Senate Armed Services Committee*, 122 CONG. REC. S11,355 (daily ed. July 1, 1976)).

90. *Id.* at 60-61.

91. *About the Committee*, *supra* note 83.

Despite these efforts to promote coordination and cross-committee information sharing, HPSCI and SSCI have not lived up to these aspirations. In 1980, Congress amended the Hughes-Ryan Act with the Intelligence Oversight Act,<sup>92</sup> which required that intelligence activities be reported to Congress before they are carried out. In exchange for these stronger reporting requirements, the Act reduced the number of committees the intelligence agencies needed to keep “fully and currently informed” from eight to two: SSCI and HPSCI.<sup>93</sup> Perhaps unintentionally, this narrowing of reporting obligations helped produce the siloed reporting regime of today, in which intelligence reporting goes to (and largely remains in) HPSCI and SSCI, and reporting of military operations is largely the province of HASC and SASC.<sup>94</sup>

The creation of siloed reporting structures continued with the 1991 Intelligence Authorization Act,<sup>95</sup> which emerged in response to the Iran-Contra affair.<sup>96</sup> The Act established the modern covert action notification requirements.<sup>97</sup> Under the law, before carrying out a covert operation, the President must determine the operation is “necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States” and set that out in a written finding.<sup>98</sup> The law further requires that the executive branch “keep the congressional intelligence committees fully and currently informed of all covert actions which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including significant failures.”<sup>99</sup> Under “extraordinary circumstances affecting vital interests of the

---

92. Intelligence Authorization Act for Fiscal Year 1981, Pub. L. No. 96-450, 94 Stat. 1975, 1981 (1980) (incorporating relevant provisions of the Intelligence Oversight Act).

93. L. ELAINE HALCHIN & FREDERICK M. KAISER, CONG. RSCH. SERV., RL32525, CONGRESSIONAL OVERSIGHT OF INTELLIGENCE: CURRENT STRUCTURE AND ALTERNATIVES 33 & n.95 (2012).

94. See *infra* Part II.B.2.

95. Intelligence Authorization Act, Fiscal Year 1991, Pub. L. No. 102-88, 105 Stat. 429 (codified at 50 U.S.C. § 3093).

96. William E. Conner, *Reforming Oversight of Covert Actions After the Iran-Contra Affair: A Legislative History of the Intelligence Authorization Act for FY 1991*, 32 VA. J. INT'L L. 871, 905 (1992).

97. Codified today at 50 U.S.C. § 3093.

98. 50 U.S.C. § 3093(a).

99. *Id.* § 3093(b)(1).

United States,” the President may notify a small group that has become known as the “Gang of Eight”—the House and Senate majority and minority leaders as well as the chairs and ranking members of HPSCI and SSCI.<sup>100</sup> According to one congressional staffer interviewed, the executive has increasingly reported activities *only* to the Gang of Eight, causing other HPSCI and SSCI members to feel that they are too often kept in the dark.<sup>101</sup> Moreover, very few, if any, staff are included in such briefings.<sup>102</sup>

Importantly, the statutory language excludes “traditional diplomatic or military activities or routine support to such activities” from these reporting requirements.<sup>103</sup> This provision exempts operations that are essentially military in nature (and thus subject to their own reporting requirements under Title 10) from intelligence oversight. In other words, Congress established two distinct categories of reporting based on formalistic, technical designations: intelligence operations, which are reported under Title 50 to HPSCI and SSCI (even when implemented by the DOD) and “traditional military activities” (TMA), which are reported under Title 10 to HASC and SASC (even when implemented by an intelligence agency).<sup>104</sup> This distinction laid the foundation for the information silos plaguing cyber and other forms of modern warfare.

## II. THE CHALLENGE OF MODERN WARFARE

Part I described the congressional committee structure for military and intelligence operations. While each set of committees has a clear jurisdictional mandate, modern warfare has increasingly blurred the lines between them. In particular, as warfare has evolved in the post-9/11 era, a number of operations have emerged at the intersection of Title 10 and Title 50 authorities. These

---

100. *Id.* § 3093(c). The Intelligence Conference Committee conferees specified at the time that “extraordinary circumstances” includes circumstances in which “the President is faced with a covert action of such extraordinary sensitivity *or risk to life* that knowledge of the covert action should be restricted to as few individuals as possible.” MARSHALL CURTIS ERWIN, CONG. RSCH. SERV., R40691, SENSITIVE COVERT ACTION NOTIFICATIONS: OVERSIGHT OPTIONS FOR CONGRESS 1-2 (2013).

101. See Interview with Congressional Staff Member #4, *supra* note 59.

102. See Interview with Congressional Staff Member #3, *supra* note 19.

103. 50 U.S.C. § 3093(e)(1)-(4).

104. See Chesney, *supra* note 11, at 595, 615-16; *id.* § 3093(e)(2).

operations could fall under the jurisdiction of multiple committees, or, in some cases, none. This is particularly evident with drone strikes, special operations, and cyber warfare. In 2013, Congress began to clarify the lines and fill oversight gaps. But its solution to the ambiguities and inconsistencies caused by the Title 10-Title 50 convergence was to assign increasing oversight responsibility to HASC and SASC, often freezing the other committees out of the oversight process.<sup>105</sup> In this Part, we explore how that process unfolded. First, we show how counterterrorism operations in the post-9/11 era increasingly blurred the Title 10/Title 50 distinction. Second, we examine the rise of multi-jurisdictional cyber operations and Congress's attempts to fill reporting gaps while reinforcing jurisdictional boundaries between the committees, thereby impeding truly effective oversight.

#### *A. The Post-9/11 Title 10-Title 50 Convergence in Modern Warfare*

The tripartite committee structure described previously might work well if the committees had truly distinct jurisdictions. When military and intelligence operations were more easily disentangled, this structure was reasonably effective. But the set of issues arising from cross-committee jurisdictions has grown substantially over the last several decades. As a result, Congress's organizational structure has become outdated. In particular, military and covert action operations have become difficult to distinguish, leading to the "Title 10-Title 50 convergence."<sup>106</sup> As one congressional staffer observed, "What consists of a Title 50 operation versus a ... Title 10 operation still isn't clear."<sup>107</sup> This phenomenon was initially observed in counterterrorism operations, especially with regard to drone strikes and special forces missions, foreshadowing later challenges for cyber oversight.

---

105. As mentioned *supra* note 33 and accompanying text, there are instances in which other committees may have a plausible claim to overseeing certain operations. In practice, however, the vast majority of modern warfare oversight is carried out by the foreign affairs/foreign relations, armed services, and intelligence committees. This Article therefore focuses on those three committees.

106. See Zoli, *supra* note 28, at 613-14, 620; Chesney, *supra* note 11, at 539, 615-16.

107. Interview with Congressional Staff Member #4, *supra* note 59.

### 1. *The Rise of Modern Warfare and Its Oversight Challenges*

These oversight challenges became particularly apparent in the wake of the 9/11 terrorist attacks. The 9/11 Commission, which was created to investigate the incident and recommend ways to prevent future attacks, stressed that executive branch reforms “will not work if congressional oversight does not change too. Unity of effort in executive management can be lost if it is fractured by divided congressional oversight.”<sup>108</sup> Calling oversight “dysfunctional,” the Commission recommended either creating a joint intelligence committee or giving the existing intelligence committees both authorizing and appropriating authorities.<sup>109</sup> In short, the Commission concluded, the outdated committee structure required reform to address contemporary cross-cutting national security challenges.

Despite these warnings, the problems the Commission identified only worsened in the years after 9/11. In particular, the convergence of Title 10 and Title 50 operations accelerated considerably. The DOD (whose operations are generally authorized under Title 10) continued to develop its clandestine capabilities for traditional military activities, while the CIA (whose operations are generally authorized under Title 50) acquired new lethal capabilities.<sup>110</sup> This convergence was especially evident with respect to operations carried out by special forces and drones. After 9/11, Special Operations Forces (SOF) became a crucial counterterrorism force. Special Operations Command (SOCOM) has more than doubled in size since 2001 and has commandos deployed to nearly 150 countries.<sup>111</sup> Likewise, lethal drone strikes have become a central element of the

---

108. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 420 (2004), <http://govinfo.library.unt.edu/911/report/911Report.pdf> [<https://perma.cc/8KT7-FFDA>] [hereinafter 9/11 COMMISSION].

109. *Id.*

110. *See Zoli, supra* note 28, at 613-14.

111. SOCOM had 33,000 personnel in 2001 and over 70,000 personnel at the start of 2020. *See* ANDREW FEICKERT, CONG. RSCH. SERV., RS21048, U.S. SPECIAL OPERATIONS FORCES (SOF): BACKGROUND AND ISSUES FOR CONGRESS 1-7 (2021). In 2009, commandos were deployed to sixty countries, and in 2015, it reached a record 147. Daniel Byman & Ian A. Merritt, *The New American Way of War: Special Operations Forces in the War on Terrorism*, 41 WASH. Q. 79, 83 (2018).

U.S. counterterrorism strategy, with one database cataloging over 14,000 strikes from 2010 to 2020.<sup>112</sup>

Security cooperation efforts, including programs to train, equip, and otherwise assist foreign defense and security forces, have also expanded significantly since 9/11.<sup>113</sup> Indeed, security cooperation formed the foundation of the U.S. counter-ISIS policy in Iraq and Syria,<sup>114</sup> and the U.S. government spent over \$200 billion on security assistance and security cooperation programs from 2006 to 2018.<sup>115</sup> In 2017, Congress authorized security cooperation funds under Title 10 U.S.C. § 127e to support special operations to combat terrorism.<sup>116</sup> One Green Beret explained, § 127e programs are “less,

112. See *Drone Warfare*, THE BUREAU OF INVESTIGATIVE JOURNALISM, <https://www.thebureauinvestigates.com/projects/drone-war> [<https://perma.cc/B8CS-9W3J>].

113. For a more expansive discussion of security cooperation, see NINA M. SERAFINO, CONG. RSCH. SERV., R44444, SECURITY ASSISTANCE AND COOPERATION: SHARED RESPONSIBILITY OF THE DEPARTMENTS OF STATE AND DEFENSE 4-5 (2016); BOLKO J. SKORUPSKI & NINA M. SERAFINO, CONG. RSCH. SERV., R44602, DOD SECURITY COOPERATION: AN OVERVIEW OF AUTHORITIES AND ISSUES 2 (2016).

114. See *Fact Sheet: Strategy to Counter the Islamic State of Iraq and the Levant (ISIL)*, WHITE HOUSE (Sept. 10, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/09/10/fact-sheet-strategy-counter-islamic-state-iraq-and-levant-isil> [<https://perma.cc/ZP8U-Z4K5>]; Tanya Somanader, *President Obama Provides an Update on Our Strategy to Degrade and Destroy ISIL*, WHITE HOUSE BLOG (July 6, 2015, 3:10 PM), <https://obamawhitehouse.archives.gov/blog/2015/07/06/president-obama-provides-update-our-strategy-degrade-and-destroy-isil> [<https://perma.cc/XP5B-SB3C>]; Bilal Y. Saab, *Broken Partnerships: Can Washington Get Security Cooperation Right?*, 42 WASH. Q. 77, 79 (2019). The Trump administration continued this emphasis on security cooperation, maintaining partnerships with over two hundred countries and international organizations to build a “robust network of allies and partners—to deter or defeat aggression by major powers,” namely Russia and China. OFF. OF THE SEC’Y OF DEF., FISCAL YEAR (FY) 2021 PRESIDENT’S BUDGET: JUSTIFICATION FOR SECURITY COOPERATION PROGRAM AND ACTIVITY FUNDING 2 (Apr. 2020), [https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021\\_Security\\_Cooperation\\_Book\\_FINAL.pdf](https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Security_Cooperation_Book_FINAL.pdf) [<https://perma.cc/QC8P-WXVY>] [hereinafter PRESIDENT’S BUDGET FY 2021].

115. See SUSAN B. EPSTEIN & LIANA W. ROSEN, CONG. RSCH. SERV., R45091, U.S. SECURITY ASSISTANCE AND SECURITY COOPERATION PROGRAMS: OVERVIEW OF FUNDING TRENDS 3 (2018). DOD requested \$7.59 billion in FY 2021. PRESIDENT’S BUDGET FY 2021, *supra* note 114, at 3. DOD requested \$9.19 billion in FY 2020 for security cooperation programs and activities. OFF. OF THE SEC’Y OF DEF., FISCAL YEAR (FY) 2020 PRESIDENT’S BUDGET: JUSTIFICATION FOR SECURITY COOPERATION PROGRAM AND ACTIVITY FUNDING 3 (Mar. 2019), [https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2020/FY2020\\_Security\\_Cooperation\\_Book\\_FINAL.pdf](https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2020/FY2020_Security_Cooperation_Book_FINAL.pdf) [<https://perma.cc/T4RH-99D6>].

116. See Wesley Morgan, *Behind the Secret U.S. War in Africa*, POLITICO (July 2, 2018, 5:08 AM), <https://www.politico.com/story/2018/07/02/secret-war-africa-pentagon-664005> [<https://perma.cc/5K97-S75C>]; Tommy Ross, *House and Senate Chart Different Courses on US Clandestine Support of Foreign Militias*, JUST SEC. (Aug. 20, 2020), <https://www.justsecurity.org/72098/house-and-senate-chart-different-courses-on-us-clandestine-support-of-foreign->

‘We’re helping you,’ and more, ‘You’re doing our bidding.’”<sup>117</sup> In 2017, SOCOM reportedly expended nearly \$80 million to resource twenty-one programs under the § 127e authority.<sup>118</sup>

As the role of special forces, drones, and security cooperation has grown, the oversight gaps caused by the artificial Title 10-Title 50 distinction have become increasingly apparent. One scholar explained, “When the CIA and SOF operate together on the battlefield, the legal distinctions regarding operating authorities and procedures, and accountability, can become blurred.”<sup>119</sup> This can have far-reaching implications for oversight.<sup>120</sup> For example, lethal operations can be carried out by either the DOD or CIA.<sup>121</sup> When led by the DOD, the operation falls under Title 10 oversight by HASC and SASC.<sup>122</sup> When led by the CIA, even with the same operators, the operation is typically undertaken as a “covert action” and

militias [<https://perma.cc/W8ZX-NXVX>].

117. Morgan, *supra* note 6.

118. See *National Defense Authorization Act for Fiscal Year 2019 and Oversight of Previously Authorized Programs: Hearing on Evolution, Transformation, and Sustainment: A Review and Assessment of the Fiscal Year 2019 Budget Request for U.S. Special Operations Forces and Command Before the Subcomm. on Emerging Threats & Capabilities of the H. Comm. on Armed Servs.*, 115th Cong. 55 (2018) (statement of General Raymond A. Thomas, III, U.S. Army Commander, U.S. Special Operations Command).

119. Philip Alston, *The CIA and Targeted Killings Beyond Borders*, 2 HARV. NAT’L. SEC. J. 283, 357 (2011) (quoting KATHRYN STONE, “ALL NECESSARY MEANS”—EMPLOYING CIA OPERATIVES IN A WARFIGHTING ROLE ALONGSIDE SPECIAL OPERATIONS FORCES 15 (2003)).

120. *Id.*

121. Initially, targeted killings were conducted largely by the CIA, but the Obama administration sought to transfer this authority to the military. See Robert Chesney, *A Revived CIA Drone Strike Program? Comments on the New Policy*, LAWFARE (Mar. 14, 2017, 12:12 PM), <https://www.lawfareblog.com/revived-cia-drone-strike-program-comments-new-policy> [<https://perma.cc/8LJU-HC9F>]. It is not clear, however, to what extent these authorities fully shifted, with some reporters claiming the DOD and CIA instead employed a hybrid approach, such as by detailing Joint Special Operations Command (JSOC) personnel to the CIA or vice versa. See Gordon Lubold & Shane Harris, *Trump Broadens CIA Powers, Allows Deadly Drone Strikes*, WALL ST. J. (Mar. 13, 2017, 6:32 PM), <https://www.wsj.com/articles/trump-gave-cia-power-to-launch-drone-strikes-1489444374> [<https://perma.cc/PJQ2-2FRG>]; Greg Miller, *Obama’s New Drone Policy Leaves Room for CIA Role*, WASH. POST (May 25, 2013), [https://www.washingtonpost.com/world/national-security/obamas-new-drone-policy-has-cause-for-concern/2013/05/25/0daad8be-c480-11e2-914f-a7aba60512a7\\_story.html?utm\\_term=.ef7d051e0b78](https://www.washingtonpost.com/world/national-security/obamas-new-drone-policy-has-cause-for-concern/2013/05/25/0daad8be-c480-11e2-914f-a7aba60512a7_story.html?utm_term=.ef7d051e0b78) [<https://perma.cc/3D7Y-LLJU>]. The Trump administration expanded the CIA’s role and responsibilities in legal strike operations and eliminated several executive branch reporting requirements. See Shannon Dick & Rachel Stohl, *U.S. Drone Policy: Transparency & Oversight*, STIMSON (Feb. 11, 2020), <https://www.stimson.org/2020/u-s-drone-policy> [<https://perma.cc/4LKK-29D9>]; Atherton, *supra* note 32.

122. See 10 U.S.C. § 127e.

subject to extensive but highly classified reporting to HPSCI and SSCI under 50 U.S.C. § 3093.<sup>123</sup> For example, the raid that killed Osama bin Laden was executed by U.S. Navy SEALs from Joint Special Operations Command (JSOC) in the DOD.<sup>124</sup> However, it was classified as a Title 50 operation under the “command” of the CIA director.<sup>125</sup> Because it was considered a CIA operation, only the Gang of Eight—which includes HPSCI and SSCI leadership as well as the House and Senate leadership—was informed. The armed services and foreign relations committees, however, were not.<sup>126</sup>

Section 127e programs and activities present further oversight challenges. While § 127e includes reporting requirements,<sup>127</sup> these operations often elude effective oversight. They are typically highly classified and briefed only to a narrow group of congressional members and staff. Former congressional staffer Tommy Ross explained, “Policymakers and congressional staffers who work in areas likely to be most affected by 127e operations—traditional foreign assistance and diplomacy activities, for example—are generally not included among those briefed ... limiting accountability and profoundly challenging the government’s ability to plan, coordinate, and integrate comprehensive assistance packages.”<sup>128</sup> Even within a single committee, only a few members are typically notified of sensitive operations, and staff are sometimes excluded altogether.<sup>129</sup>

Moreover, similar and sometimes overlapping training and assistance programs can be operated by the CIA, which follows its own distinct reporting regime.<sup>130</sup> For example, the CIA reportedly spent over \$1 billion over four years on a covert action program to support Syrian rebels.<sup>131</sup> This program reportedly operated alongside an

123. See LARRY LEWIS & DIANE VAVRICHEK, *RETHINKING THE DRONE WAR* 210-11 (2016), <https://fas.org/man/eprint/drone-war.pdf> [<https://perma.cc/8M9T-28Z8>].

124. Nicholas Schmidle, *Getting Bin Laden*, *NEW YORKER* (Aug. 1, 2011), <https://www.newyorker.com/magazine/2011/08/08/getting-bin-laden> [<https://perma.cc/F5PW-K25B>].

125. See JOHN ROLLINS, *CONG. RSCH. SERV.*, R41809, *OSAMA BIN LADEN’S DEATH: IMPLICATIONS AND CONSIDERATIONS* 1, 1 (2011).

126. See *id.*

127. 10 U.S.C. § 127e(d)(1), (h)(3).

128. Ross, *supra* note 116; see also MARTHA LEE, ALEXANDRA SCHMITT, & GABRIELLE TARINI, *PARTNERING TO PROTECT* 63 (2019).

129. See Interview with former Congressional Staff Member #6, *supra* note 7.

130. See LEWIS & VAVRICHEK, *supra* note 123, at 210-11.

131. See Mark Mazzetti, Adam Goldman & Michael S. Schmidt, *Behind the Sudden Death of a \$1 Billion Secret C.I.A. War in Syria*, *N.Y. TIMES* (Aug. 2, 2017), <https://www.nytimes.com/>

overt DOD program authorized and overseen by HASC and SASC.<sup>132</sup> The CIA programs would have been reported under Title 50 to HPSCI and SSCI alone, even though they may have directly overlapped, and even competed, with programs authorized by HASC and SASC.<sup>133</sup> As one former staffer put it in an interview with us, “I saw in a couple of cases some of these programs that were not only duplicative, but competitive. The DOD and CIA were trying to displace one another from the same landscape.”<sup>134</sup>

Importantly, special operations, drone strikes, and security cooperation missions often fall outside of the oversight jurisdiction of HFAC and SFRC under the WPR. As discussed in Part I,<sup>135</sup> the executive branch has often narrowly defined “hostilities” in the WPR to require “the presence of U.S. ground troops, U.S. casualties or a serious threat thereof.”<sup>136</sup> This definition “allows the President to escape the WPR whenever drones are relied upon—regardless of the extent of a military campaign involving drones.”<sup>137</sup> Under this contested interpretation of hostilities, the executive branch is not obligated to report special forces operations, including kill/capture missions, to Congress under the WPR.<sup>138</sup> This interpretation has largely kept HFAC and SFRC in the dark on the vast majority of counterterrorism operations.

---

2017/08/02/world/middleeast/cia-syria-rebel-arm-train-trump.html [https://perma.cc/587E-Q2PL].

132. See CHRISTOPHER M. BLANCHARD & AMY BELASCO, CONG. RSCH. SERV., R43727, TRAIN AND EQUIP PROGRAM FOR SYRIA: AUTHORITIES, FUNDING, AND ISSUES FOR CONGRESS 1, 9 (2015).

133. See LEWIS & VAVRICHEK, *supra* note 123, at 210-11.

134. Interview with former Congressional Staff Member #6, *supra* note 7.

135. See *supra* Part I.A.

136. See Benjamin R. Farley, *Drones and Democracy: Missing Out on Accountability?*, 54 S. TEX. L. REV. 385, 416 (2012).

137. *Id.* at 417.

138. Many continue to maintain that the “hostilities” bar is not nearly so high and that, at a minimum, lethal operations that put U.S. troops in harm’s way—including special operations and security cooperation missions—fall under the WPR’s notification requirements. See, e.g., Jensen, *supra* note 60, at 535-37.

## 2. Congress's Attempts to Respond to the Challenges of Modern Warfare

Starting in 2013, Congress began to fill the oversight gaps caused by the Title 10-Title 50 convergence. HASC and SASC leveraged the NDAA process to clarify special operations reporting procedures and consolidate their jurisdiction.<sup>139</sup> Through the FY 2014 NDAA process, Congress defined “sensitive military operation[s]” (SMOs), now codified under 10 U.S.C. § 130f.<sup>140</sup> This statute requires the Secretary of Defense to “promptly” notify the defense committees (HASC, SASC, House Appropriations Defense Subcommittee (HAC-D), and Senate Appropriations Defense Subcommittee (SAC-D)) of any “lethal operation or capture operation conducted by the armed forces ... outside a theater of major hostilities.”<sup>141</sup> The Secretary must also “periodically brief the congressional defense committees on [DOD] personnel and equipment assigned to sensitive military operations.”<sup>142</sup> Robert Chesney described the statute as “analogous to the more-familiar oversight system we already have for Title 50 covert action,” observing that “the new SMO oversight architecture

---

139. See Craig Whitlock, *Lawmaker Wants Military to Promptly Alert Congress About Drone Strikes*, WASH. POST (May 8, 2013), [https://www.washingtonpost.com/world/national-security/lawmaker-wants-military-to-promptly-alert-congress-about-drone-strikes/2013/05/08/dcc73068-b817-11e2-bd07-b6e0e6152528\\_story.html?hpid=z3](https://www.washingtonpost.com/world/national-security/lawmaker-wants-military-to-promptly-alert-congress-about-drone-strikes/2013/05/08/dcc73068-b817-11e2-bd07-b6e0e6152528_story.html?hpid=z3) [<https://perma.cc/M53F-EUSW>]; Sydney J. Freedberg Jr., *Thornberry Bill “Lets Congress Push Back” on Drone Strikes, Special Ops*, BREAKING DEF. (May 13, 2013, 2:50 PM), <https://breakingdefense.com/2013/05/thornberry-bill-lets-congress-push-back-on-drone-strikes-special-ops-not-declared-wars/> [<https://perma.cc/N3HK-U9BM>].

140. National Defense Authorization Act for Fiscal Year 2014, Pub. L. No. 113-66, § 1041, 127 Stat. 672, 856-57 (2013) (codified as amended at 10 U.S.C. § 130f) [hereinafter FY 2014 NDAA].

141. *Id.* § 1041(a), (d) (codified as amended at 10 U.S.C. § 130f(a)). The definition of “sensitive military operation” was updated in subsequent NDAAAs. See John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1031(a), 132 Stat. 1636, 1953 (2018) [hereinafter FY 2019 NDAA]; National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 1036(d), 130 Stat. 2000 (2016) [hereinafter FY 2017 NDAA]. The statute no longer provides that the operation must be “outside a theater of major hostilities,” but defines a sensitive military operation as “(A) a lethal operation or capture operation conducted by the armed forces or conducted by a foreign partner in coordination with the armed forces that targets a specific individual or individuals; or (B) an operation conducted by the armed forces in self-defense or in defense of foreign partners.” 10 U.S.C. § 130f(d)(1). The statute expressly excludes operations in Afghanistan, Syria, or Iraq from the definition of a sensitive military operation. *Id.* § 130f(d)(2).

142. *Id.* § 130f(c).

helps minimize oversight dropoff when it is JSOC rather than CIA that is conducting a kill/capture mission outside the 'hot battlefield' areas."<sup>143</sup> In short, 10 U.S.C. § 130f minimized the daylight between oversight over similar operations conducted by the intelligence community and the DOD. In addition to requiring one-off notifications of SMOs, the FY 2014 NDAA also required quarterly counterterrorism briefings, codified at 10 U.S.C. § 485.<sup>144</sup>

In the process of remedying the ambiguities and inconsistencies caused by the Title 10-Title 50 convergence, HASC and SASC also consolidated their jurisdiction over those operations. The new reporting requirements ended debate over whether these clandestine, "below the threshold" operations needed to be reported to the foreign relations committees under the WPR or to the intelligence committees under the covert action statute. Unless conducted as part of ongoing hostilities, they would be reported only to the armed services committees.

Congress continued to amend and clarify this reporting structure over the next six years, creating a complex but relatively robust oversight regime. While these changes allowed Congress to address emerging threats and capabilities, they also further entrenched information silos. For example, the FY 2017 NDAA clarified the requirement for "prompt" reporting by adding specific deadlines. The new statute required notification of SMOs to the armed services committees within forty-eight hours of the operation and "immediate" notification in the event of an unauthorized disclosure.<sup>145</sup> The statute also mandated notification within fourteen days if the DOD sought to change any reporting procedures. The same NDAA also addressed a new ambiguity in whether self-defense operations should be considered SMOs. In multiple out-of-theater countries,

---

143. Robert Chesney, *Expanding Congressional Oversight of Kill/Capture Ops Conducted by the Military: Section 1036 of the NDAA*, LAWFARE (Dec. 8, 2016, 6:25 PM), <https://www.lawfareblog.com/expanding-congressional-oversight-killcapture-ops-conducted-military-section-1036-ndaa> [<https://perma.cc/BGJ9-XB2F>].

144. FY 2014 NDAA, *supra* note 140, § 1042. These briefings must outline the DOD's "counterterrorism operations and related activities," including updates on activities within each geographic combatant command and how they relate to the respective theater campaign plan, relevant legal authorities and issues, and related interagency initiatives. 10 U.S.C. § 485(b)(1)-(3).

145. FY 2017 NDAA, *supra* note 141, § 1036(a)-(b) (codified as amended at 10 U.S.C. § 130f).

but especially Somalia, the Obama administration had been justifying kinetic strikes as either self-defense or “collective self-defense” of U.S. partner forces.<sup>146</sup> In turn, Congress explicitly expanded the definition of SMO to include not only kill/capture missions but also the use of force in self-defense or in defense of foreign partners.<sup>147</sup>

These amendments, enacted in response to gaps and ambiguities as they arose, have created an oversight regime that is comprehensive but has consolidated oversight of SMOs under the armed services committees’ jurisdiction. This has led to a somewhat bizarre situation in which only the armed services committees receive reporting on SOCOM-led operations and drone strikes; only the intelligence committees are notified of parallel operations led by the CIA; and the foreign relations committees are often not informed of either type of operation, despite their role in overseeing war powers reporting, country missions, and diplomatic relations, as well as authorizing uses of force, all of which can be directly impacted by such operations.<sup>148</sup> One former congressional staff member recalled that while putting together a “massive Pakistan aid package that would shift the basis of U.S.-Pakistan relations,” committee members were not read in on the United States’ drone program in the country.<sup>149</sup> Another former congressional staffer explained, “The siloing issue can be an even bigger problem in the counterterrorism kinetic world of special forces and CIA operations against terrorists.”<sup>150</sup> As we shall see in the next Section, similar coordination failures plague the cyber oversight regime.

---

146. Charlie Savage, Eric Schmitt & Mark Mazzetti, *Obama Expands War with Al Qaeda to Include Shabab in Somalia*, N.Y. TIMES (Nov. 27, 2016), <https://www.nytimes.com/2016/11/27/us/politics/obama-expands-war-with-al-qaeda-to-include-shabab-in-somalia.html> [<https://perma.cc/U67B-8QYU>] (“Over the past year, the military has routinely invoked a built-in exception to those rules for airstrikes taken in ‘self-defense,’ which can include strikes to help foreign partners even when Americans are not at direct risk.”); see also E. L. Gaston, *Reconceptualizing Individual or Unit Self-Defense as a Combatant Privilege*, 8 HARV. NAT’L SEC. J. 283, 328-29 (2017).

147. The same amendment also sought to simplify the definition of SMO. See 10 U.S.C. § 130f(d).

148. If the activities are undertaken as part of ongoing hostilities, they would be captured in 50 U.S.C. § 1543(c) reporting.

149. Interview with Congressional Staff Member #4, *supra* note 59.

150. Interview with Congressional Staff Member #5, *supra* note 22.

Table 1: Key Counterterrorism Operations Oversight Provisions<sup>151</sup>

<b>Special Operations, Drone Strikes, and Targeted Killings</b>		
<b>Provision</b>	<b>Requirement</b>	<b>Recipient</b>
10 U.S.C. § 485	Monthly briefings by DOD on counterterrorism operations.	HASC; SASC
10 U.S.C. § 130f	Written notice of “sensitive military operations” within 48 hours of the operation.	HASC; SASC
FY 2018 NDAA § 1057	Annual report on civilian casualties caused by U.S. military operations.	HASC; SASC
FY 2020 NDAA § 1723	Annual joint report by the Director of National Intelligence (DNI) and the Secretary of Defense on strikes against terrorist targets outside areas of hostilities, and assessments of combatant and noncombatant deaths from those strikes.	“Congress”
10 U.S.C. § 127e	Notification within 15 days, or within 48 hours if “extraordinary circumstances ... impact[] national security,” of initiating an operation that supports “foreign forces, irregular forces, groups, or individuals engaged in supporting or facilitating authorized ongoing military operations by United States special operations forces to combat terrorism”; biannual reports on § 127e operations.	HASC; SASC

151. All provisions in Table 1—except 50 U.S.C. § 3093—also require reporting to the House and Senate appropriations committees.

50 U.S.C. § 3093	Report a presidential finding authorizing a covert action before initiating the operation; keep committees “fully and currently informed of all covert actions,” including significant changes to previously approved covert action.	HPSCI; SSCI
------------------	--	-------------

## B. Congressional Oversight of Cyber Operations

### 1. Early Responses to the Emerging Cyber Domain

Around the same time that Congress pursued comprehensive reform of oversight over special operations and drone strikes, it began crafting a legal regime for cyber operations. Like special forces missions and drone strikes, cyber operations blurred the distinction between Title 10 and Title 50, creating challenges for both Congress and the White House. Cyber operations, like counterterrorism operations, do not map neatly onto the existing, distinct reporting requirements under the WPR, the Title 10 regime for traditional military activities, or the Title 50 covert action statute.

Congress’s initial oversight efforts focused on developing an understanding of this new domain and the executive branch’s cyber strategy. The United States’ vulnerability to potentially devastating cyber operations became increasingly apparent.<sup>152</sup> Observers warned that the United States lacked a strategy for deterring cyber attacks and deploying offensive cyber capabilities.<sup>153</sup> In 2009, the Secretary

152. David E. Sanger, John Markoff & Thom Shanker, *U.S. Steps Up Effort on Digital Defenses*, N.Y. TIMES (Apr. 27, 2009), [https://www.nytimes.com/2009/04/28/us/28cyber.html?\\_r=2](https://www.nytimes.com/2009/04/28/us/28cyber.html?_r=2) [<https://perma.cc/L3EP-PXB4>].

153. For example, the Center for Strategic and International Studies raised the alarm in four reports between 2008 and 2011, warning that “America’s failure to protect cyberspace is one of the most urgent national security problems facing the [Obama] administration.” CTR. FOR STRATEGIC & INT’L STUD., *SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 11* (2008), [https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/media/csis/pubs/081208\\_securingcyberspace\\_44.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf) [<https://perma.cc/EEL9-HEVE>]; CTR. FOR STRATEGIC & INT’L STUD., *CYBERSECURITY TWO YEARS LATER 1* (2011) (observing that 2010 alone saw major cyber-attacks on Google and the DOD, the stuxnet attack on Iranian centrifuges, and denial-of-service attacks on Wikileaks), [https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/publication/110128\\_Lewis\\_CybersecurityTwoYearsLater\\_Web.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf) [<https://perma.cc/ZZH3-NCNZ>]; see also Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Niz,

of Defense established Cyber Command as a subordinate command under U.S. Strategic Command to elevate cyber operations within the military and strengthen the Department's cyber capabilities.<sup>154</sup> A year later, Congress directed the Pentagon to submit a report on its "cyber warfare policy."<sup>155</sup> In its response, the DOD stated that it would conduct "offensive cyber operations" consistent with the policy and legal principles governing kinetic capabilities.<sup>156</sup> It also made clear its view that few, if any, cyber operations would trigger the WPR on their own.<sup>157</sup> This meant, of course, that its activities would remain outside the purview of the foreign relations committees and solely within the oversight authority of the armed services committees.

While Cyber Command's efforts to disrupt terrorist organizations in war zones were relatively uncontroversial, its attempts to carry out offensive operations beyond active combat zones or areas of hostilities—such as those that touched networks or servers within third-party countries—prompted heated debate within the executive branch about the proper home for these activities.<sup>158</sup> Cyber Command argued that these clandestine operations were properly considered Title 10 "traditional military activities" even if outside traditional war zones because of the difficulties in defining the battlespace when it comes to cyber activities.<sup>159</sup> Seeking to limit Cyber Command's turf, the CIA argued that offensive cyber operations beyond the battle zone fell under its purview as covert action—requiring a presidential finding and compliance with Title

---

Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 821 (2012) (defining cyber-attack).

154. Memorandum from Off. of Sec'y of Def., Memorandum for Secretaries of the Military Departments, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009), <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf> [<https://perma.cc/62AR-YUJ6>].

155. Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111-383, § 934, 124 Stat. 4338-39 (2011).

156. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011 5 (2011), <https://www.hsdl.org/?abstract&did=692701> [<https://perma.cc/83U6-LTYG>].

157. *Id.* at 9.

158. Interview with Congressional Staff Member #5 (Jan. 21, 2021), *supra* note 22.

159. Ellen Nakashima, *Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield*, WASH. POST (Nov. 6, 2010, 12:41 AM), <https://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html> [<https://perma.cc/Z7J6-MCD4>].

50's reporting provisions.<sup>160</sup> The State Department similarly favored cabining Cyber Command's authorities, reportedly fearing diplomatic backlash from affected third-party countries.<sup>161</sup>

In the FY 2012 NDAA, Congress weighed in on this debate, affirming the DOD's authority to "conduct offensive operations in cyberspace to defend our Nation, Allies and interests."<sup>162</sup> In the conference report, Congress noted the "lack of historical precedent for what constitutes traditional military activities in relation to cyber operations," yet also acknowledged the need "to undertake offensive military cyber activities, including where the role of the United States Government is not apparent or to be acknowledged."<sup>163</sup> Congress did not resolve the military activity-covert action dispute, but it emphasized that cyber operations must be consistent with the legal and policy regimes for kinetic capabilities.<sup>164</sup>

As these debates continued, Congress took initial steps to establish a framework for continuous oversight over cyber operations. SASC had reportedly expressed concerns in early 2011 that the DOD was not including cyber activities in its quarterly report on clandestine military activities.<sup>165</sup> In the FY 2013 NDAA, Congress filled this reporting gap by enacting what is today's most central cyber reporting requirement: the DOD's obligation to provide quarterly briefings to the armed services committees "on all offensive and significant defensive military operations in cyberspace."<sup>166</sup> By including this provision as part of its efforts to "address[] adversarial use of the internet as a new battlespace," legislators sought to "maintain[] a focus on increasing oversight of cyberspace

160. *Id.*

161. *Id.*; see also Chesney, *supra* note 11, at 627 (arguing that the Title 10-Title 50 debate in the context of cyber operations not only concerns authorization and reporting requirements, but also implicates substantive legal issues, such as the protection of sovereignty under international law).

162. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011) [hereinafter FY 2012 NDAA].

163. H.R. REP. NO. 112-329, at 686 (2011) (Conf. Rep.).

164. FY 2012 NDAA, *supra* note 162, § 954.

165. *Senators Say Military Cyber Ops Not Disclosed*, FOX NEWS (Mar. 20, 2015), <https://www.foxnews.com/us/senators-say-military-cyber-ops-not-disclosed.amp> [<https://perma.cc/Y6W3-2B5D>].

166. National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 939(a), 126 Stat. 1632, 1888 (codified as amended at 10 U.S.C. § 484(a)) [hereinafter FY 2013 NDAA].

operations, as well as fostering a better understanding of the challenges facing the Department when operating in cyberspace.”<sup>167</sup> This foundational reporting requirement fell exclusively under the armed services committees’ jurisdiction, laying the foundation for a recurring trend as cyber oversight requirements evolved.<sup>168</sup> According to a former SFRC senior staff member, there was no real effort to include the foreign relations committees in these quarterly briefings nor in any intelligence committee briefings on related matters, despite the foreign relations committees’ jurisdiction over war powers. Any attempt would have likely been futile, the staff member explained: “If [HFAC and SFRC] couldn’t get operational access to military or intelligence operations generally, cyber would be even harder.”<sup>169</sup>

## 2. *Filling Gaps While Entrenching Silos*

According to a congressional staff member involved in cyber oversight deliberations at the time, the armed services committees were initially concerned about preventing Cyber Command from exceeding its authorities and acting like a “bull in a china shop.”<sup>170</sup> However, these concerns turned out to be unwarranted. In the first few years of its existence, Cyber Command employed a highly cautious approach to cyber warfare. U.S. military cyber operations remained relatively limited to theaters of active combat, and fears that Cyber Command would assume an aggressive cyber posture without any legal or regulatory constraints did not materialize.<sup>171</sup> For several years after Cyber Command’s inception, oversight over cyber operations thus remained an “academic issue,” the staff member recalled.<sup>172</sup> The DOD’s incomplete efforts at articulating a cyber strategy, limited proactive operations, and the rapid rise of cyber adversaries explain why Congress both empowered the DOD in cyberspace and simultaneously demanded more reporting.

---

167. H. COMM. ON ARMED SERVS., REP. ON H.R. 4310, H.R. REP. NO. 112-479, pt. 1, at 4 (2012) (FY 2013 NDAA).

168. FY 2013 NDAA, *supra* note 166, § 939(a).

169. *See* Interview with Jamil N. Jaffer, *supra* note 27.

170. Interview with Congressional Staff Member #5, *supra* note 22.

171. *Id.*

172. *Id.*

Over the next several years, the armed services committees continued to build out the legal framework for cyber operations through the NDAA with two oversight goals in mind: first, ensuring that legislators were kept apprised of the executive branch's cyber operations; and second, compelling the DOD to articulate a robust cyber strategy and empowering it to act in cyberspace. Regarding the former objective, the armed services committees mandated the DOD disaggregate its reporting by geographic and functional command and include relevant legal authorities and limitations.<sup>173</sup> As Cyber Command matured and the DOD assumed a more proactive cyber posture, particularly with the advent of its "Defend Forward" strategy,<sup>174</sup> these reporting and notification requirements became essential to Congress's efforts to oversee the executive branch. As a staff member expressed, the "NDAA has had the greatest impact in terms of enabling the DOD to take a more active role in defending against cyber intrusions."<sup>175</sup>

Congress also leveraged the NDAA process to urge the DOD to increase engagement in cyberspace. Between 2013 and 2017, in the wake of a series of high-profile cyber incidents, HASC and SASC grew increasingly dissatisfied with the DOD's untransparent and uncoordinated efforts to deter cyber aggression by adversaries such as Russia, China, Iran, and North Korea.<sup>176</sup> Amendments to the

---

173. See 10 U.S.C. § 484(b)(1)-(2). In addition, the quarterly briefings must also include related interagency activities under 10 U.S.C. § 484(b)(3) and readiness assessments of DOD cyber personnel under 10 U.S.C. § 484(b)(4). See Oona A. Hathaway, Tobias Kuehne, Randi Michel & Nicole Ng, Appendix A: Cyber Operations, <https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/BXRA9I> [<https://perma.cc/Z5RW-2XQZ>] [hereinafter Appendix A: Cyber Operations] (online appendix to this Article cross-walking congressional reporting requirements).

174. See *infra* notes 210-12 and accompanying text.

175. Interview with Congressional Staff Member #2 (Oct. 7, 2020).

176. See, e.g., S. REP. NO. 112-173, at 480-81 (2012) (FY 2013 NDAA) (dissenting view complaining that NDAA should have included a call for articulating a strategy); S. REP. NO. 113-44, at 160 (2013) (FY 2014 NDAA) ("The committee has been pressing for a strategy and doctrine for deterring adversaries from attacking the United States and our allies for years. The administration has made some progress in this area, producing some elements of such a strategy, but the depth and breadth of the analysis and explanation of the U.S. posture needs to be significantly improved."); S. REP. NO. 114-49, at 264 (2015) (FY 2016 NDAA) ("The committee is also concerned that failing to impose meaningful consequences on those seeking to harm the United States through the cyber domain will embolden our adversaries and lead to more severe attacks in the future."); S. REP. NO. 115-125, at 296 (2017) (FY 2018 NDAA) ("The committee recommends a provision that would establish the policy of the United States

NDAA expressly required the executive branch to articulate its “policy to deter adversaries in cyberspace.”<sup>177</sup> During the FY 2017 NDAA drafting process, SASC expressed that DOD policy reports were delayed and inadequate.<sup>178</sup> The next year, the FY 2018 NDAA imposed a spending restriction on DOD funds until submission of a national policy on cyberspace, cybersecurity, and cyber warfare.<sup>179</sup> Importantly, the President was required to transmit this report—and a subsequent report required by the FY 2019 NDAA—not only to the armed services committees, but also to the foreign relations, judiciary, and homeland security committees.<sup>180</sup> Congress also required the executive branch to conduct an interagency cyber posture review for the next five to ten years to “clarify” U.S. cyber deterrence “policy and strategy,”<sup>181</sup> which later became a quadrennial requirement.<sup>182</sup>

As the DOD’s cyber capabilities expanded and the possibility that operations would be conducted outside of areas of active hostilities grew, Congress concluded that it needed more prompt and active reporting on the DOD’s military cyber activities.<sup>183</sup> Congress therefore supplemented the quarterly briefing requirement for cyber operations, establishing the most significant reporting requirements for cyber operations to date.<sup>184</sup> Through the FY 2018 NDAA, Congress

---

with respect to matters pertaining to cyberspace, cybersecurity, and cyber warfare. The committee has long expressed its concern with the lack of an effective strategy and policy for addressing cyber threats and cyber deterrence.”)

177. FY 2014 NDAA, *supra* note 140, § 941; *see also* National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 1646, 129 Stat. 726, 1117-18 (2015) [hereinafter FY 2016 NDAA]; FY NDAA 2017, *supra* note 141, § 1654; National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1633, 131 Stat. 1283, 1738-39 (2017) (codified as amended at 10 U.S.C. § 130g) [hereinafter FY 2018 NDAA].

178. *See* S. REP. NO. 114-255, at 349 (2016) (criticizing the cyber deterrence policy report required by § 941 of the FY 2014 NDAA for “disappointingly repackag[ing] the same rhetoric and recycl[ing] the same pronouncements that have failed to impose any consequences on those seeking to undermine the national security of the United States in cyberspace”).

179. *See* FY 2018 NDAA, *supra* note 177, § 1633(c)(1) (withholding 40 percent of funds for the Defense Information Systems Agency until the submission of the report).

180. *See id.* § 1633; FY 2019 NDAA, *supra* note 141, § 1636. Only the 2019 report was required to be transmitted to the intelligence committees.

181. *See* FY 2018 NDAA, *supra* note 177, § 1644.

182. *See* National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1635, 133 Stat. 1198, 1748 (2019) (codified as amended at 10 U.S.C. § 394) [hereinafter FY 2020 NDAA].

183. *See id.*

184. *See* Press Release, Rep. Jim Langevin (D-RI), House of Representatives, Langevin,

created a specific notification regime.<sup>185</sup> To stay informed of armed forces operations that were “intended to cause cyber effects outside a geographic location” of U.S. hostilities (as defined by the WPR),<sup>186</sup> Congress required the Secretary of Defense to notify HASC and SASC within forty-eight hours of any “sensitive military cyber operation” (SMCO).<sup>187</sup> This included both offensive and defensive cyber operations.<sup>188</sup> The reporting regime, codified today at 10 U.S.C. § 395, exempted covert action and cyber operations conducted in areas of active hostilities (for example, Iraq, Syria, and Afghanistan) and mirrored the SMO notification and reporting regime that Congress had instituted four years prior for special operations forces.<sup>189</sup> As HASC ranking member Adam Smith explained, the framework drew on “lessons ... learned from the oversight of more traditional DOD sensitive activities outside of areas of active hostilities” to “establish clear standards, processes, and procedures for notification to Congress of sensitive operations.”<sup>190</sup> The FY 2018 NDAA also established a forty-eight-hour notification requirement for “[t]he use as a weapon of any cyber capability” approved under international law, as well as a quarterly reporting on the DOD’s weapons review process for cyber weapons.<sup>191</sup> This reporting, too, went only to the armed services committees.<sup>192</sup>

---

Smith, Thornberry, and Stefanik Introduce Bipartisan Cyber Legislation (June 8, 2017), <https://langevin.house.gov/press-release/langevin-smith-thornberry-and-stefanik-introduce-bipartisan-cyber-legislation> [<https://perma.cc/8339-PYRY>].

185. See FY 2018 NDAA, *supra* note 177, § 1631(a) (initially codified at 10 U.S.C. § 130j, then renumbered as 10 U.S.C. § 395); see also Appendix A: Cyber Operations, *supra* note 173.

186. 10 U.S.C. § 395(c)(1)(A)-(B).

187. *Id.* § 395(b)(3).

188. *Id.* § 395. One item that was relieved of the forty-eight-hour reporting requirement was DOD-internal legal reviews of whether to use a cyber capability as a novel weapon. See *id.* § 396(a)(1). “[R]ecogniz[ing] that providing Congress with each individual legal review of a cyber capability intended for use as a weapon could become[ ] burdensome,” the Senate and House committees agreed to require aggregate reports every quarter. H.R. REP. NO. 115-404, at 1017 (2017) (Conf. Rep.) (FY 2018 NDAA). The provision is codified at 10 U.S.C. § 396(a)(1). However, the postapproval use of such a capability must be reported within forty-eight hours. See *id.* § 396(a)(2). Training exercises and covert actions are exempted. See *id.* § 396(c).

189. See *supra* Part II.A.2.

190. See Press Release, *supra* note 184.

191. FY 2018 NDAA, *supra* note 177, § 1631 (codified as amended at 10 U.S.C. § 130k).

192. *Id.*

The next year, Congress made even more consequential changes. The FY 2019 NDAA attempted to resolve the Title 10-Title 50 debate and remove bureaucratic hurdles that had hampered Cyber Command's operations.<sup>193</sup> These reforms came in the wake of Russia's use of information and cyber operations during the 2016 election and in the run up to the 2018 midterms, which prompted widespread frustration over Cyber Command's perceived limited ability to deter adversaries.<sup>194</sup> As the FY 2019 NDAA conference report explained, the DOD "routinely confronted" the challenge of deciding whether "clandestine military activities" were "traditional military activities" or "covert actions requiring a presidential finding" under Title 50.<sup>195</sup> Thus, before taking any clandestine action outside combat zones, Cyber Command had to "tease out why cyber operations were [traditional military activities]."<sup>196</sup> This limited the DOD to "actions that could be conducted overtly on attributable infrastructure without deniability—an operational space that is far too narrow to defend national interests."<sup>197</sup> Moreover, Presidential Policy Directive-20 (PPD-20), issued by President Obama, required interagency review and approval for any offensive cyber operation to manage any collateral consequences, such as interference with intelligence activities.<sup>198</sup> Congress criticized PPD-20 for causing "the executive branch to ha[ve] squandered years in interagency deliberations."<sup>199</sup>

Congress attempted a legislative fix through the FY 2019 NDAA. As a congressional staff member recalled, "Congress has been one of the most active in pushing [the DOD] to include a more offensive approach ... we wanted to make sure the Department had the authorities to go out and do those activities."<sup>200</sup> Thus, § 1632 made it

---

193. See FY 2019 NDAA, *supra* note 141, § 1631 (codified as amended at 10 U.S.C. § 394(c), (f)).

194. See Interview with Congressional Staff Member #5, *supra* note 22.

195. H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.) (FY 2019 NDAA).

196. Interview with U.S. Department of Defense Lawyer (Jan. 14, 2021).

197. H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.) (FY 2019 NDAA).

198. Memorandum from President Barack Obama to Vice President et al. 9 (Oct. 2012), <https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf> [<https://perma.cc/3L7G-SXSF>] (detailing President Obama's Presidential Policy Directive 20 (PPD-20)).

199. H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.).

200. Interview with Congressional Staff Member #2, *supra* note 175; see also Loch K. Johnson, *The Church Committee Investigation of 1975 and the Evolution of Modern*

emphatically clear that clandestine cyber military activities,<sup>201</sup> including operations “short of hostilities” or generating effects outside areas of hostilities, fall under the traditional military activities exception to covert action and are thus exclusively subject to Title 10 oversight by the armed services committees.<sup>202</sup> Thus, even cyber operations conducted in secrecy without public acknowledgement were defined as TMA, allowing Cyber Command to pursue deniable operations without the more demanding Title 50 covert action requirements. In the words of a congressional staff member, § 1632 “was an explicit repudiation of objections that other agencies and departments had always put up to challenge DOD conducting operations in cyberspace.”<sup>203</sup> Section 1632 effectively closed the door on arguments that the intelligence committees should exercise oversight over clandestine cyber operations.

To resolve any doubt about the DOD’s authorities and urge a response to “continuous aggression” by adversaries, Congress also expressly authorized cyber operations against Russia, China, North Korea, and Iran.<sup>204</sup> Section 1642 of the FY 2019 NDAA provided that in response to an “active, systematic, and ongoing campaign of attacks ... including attempting to influence American elections and democratic political processes” by any one of these countries, the National Command Authority (that is, the President and the Secretary of Defense) could authorize the Secretary of Defense via Cyber Command “to take appropriate and proportional action in

---

*Intelligence Accountability*, 23 INTEL. & NAT’L SEC. 198, 217 (2008) (describing the armed services committees as taking on a “cheerleading role” in overseeing the DOD’s cyber operations).

201. Section 1632(f) defines a “clandestine military activity or operation in cyberspace” as one that

(A) is marked by, held in, or conducted with secrecy, where the intent is that the activity or operation will not be apparent or acknowledged publicly; and “(B) is to be carried out—(i) as part of a military operation plan approved by the President or the Secretary in anticipation of hostilities or as directed by the President or the Secretary; “(ii) 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 “(iii) in support of information related capabilities.

FY 2019 NDAA, *supra* note 141, § 1632(f)(1).

202. FY 2019 NDAA, *supra* note 141, §§ 1631(b), 1632 (codified as amended at 10 U.S.C. § 394(c), (f) (2020)).

203. Interview with Congressional Staff Member #5, *supra* note 22.

204. H.R. REP. NO. 115-874, at 1055 (2018) (Conf. Rep.).

foreign cyberspace to disrupt, defeat, and deter such attacks ... as traditional military activities.”<sup>205</sup>

Observers have called § 1642 a “mini-cyber AUMF.”<sup>206</sup> However, the NDAA requires routine reporting of these operations (notification under 10 U.S.C. § 395 and quarterly briefings) only to the armed services committees, excluding the foreign relations committees, which have jurisdiction over AUMFs.<sup>207</sup> Indeed, because the provision was included in the NDAA, the foreign relations committees were excluded from its drafting—again, even though AUMFs formally fall within their exclusive jurisdiction.<sup>208</sup> There was, however, a modest nod in the new legislation to the interests of the foreign relations committees and intelligence committees: the DOD is required to submit an annual report concerning cyber attacks by Russia, China, North Korea, and Iran to the foreign affairs, intelligence, and armed services committees, as well as “adjustments of the Department of Defense in the response directed or recommended by the Secretary.”<sup>209</sup>

Congress’s efforts complemented parallel changes in the executive branch’s approach to cyber operations. In September 2018, the DOD publicly announced “Defend Forward,”<sup>210</sup> a strategy involving persistently engaging adversaries outside of the DOD’s own networks by “impos[ing] tactical friction and strategic costs on our adversaries” closer to their home networks.<sup>211</sup> In other words, Cyber Command began to more proactively target adversaries’ computer

205. FY 2019 NDAA, *supra* note 141, § 1642(a)(1).

206. See 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> [<https://perma.cc/5K2B-2DWL>].

207. FY 2019 NDAA, *supra* note 141, § 1642(a)(2); see also *supra* notes 44-47 and accompanying text.

208. See *supra* notes 44-47 and accompanying text.

209. FY 2019 NDAA, *supra* note 141, § 1642(c); see also Appendix A: Cyber Operations, *supra* note 173. The Act also makes clear that nothing in the new legislation “may be construed to ... affect the War Powers Resolution.” FY 2019 NDAA, *supra* note 141, § 1642(d)(2).

210. Mark Pomerleau, *Here’s How Cyber Command is Using “Defend Forward,”* FIFTH DOMAIN (Nov. 12, 2019), <https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward> [<https://perma.cc/KS2D-VD9Y>].

211. ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY: COMMAND VISION FOR U.S. CYBER COMMAND 6 (2018); see also Gary Corn, *Solar Winds is Bad, But Retreat From Defend Forward Would Be Worse*, LAWFARE (Jan. 14, 2021, 11:01 AM), <https://www.lawfareblog.com/solar-winds-bad-retreat-defend-forward-would-be-worse> [<https://perma.cc/QRU8-JCJN>].

networks, hunting for and disrupting planned malicious activity, attempting “to disrupt or halt malicious cyber activity at its source.”<sup>212</sup> To operationalize this strategy, President Trump issued National Security Presidential Memorandum-13 (NSPM-13), which replaced PPD-20 and the interagency process that Congress had excoriated, creating a streamlined approval process for cyber missions.<sup>213</sup> On Election Day in 2018, for example, Cyber Command used these new authorities to cut off the internet access of the Kremlin-linked Internet Research Agency, a Russian troll factory that had targeted the 2016 election.<sup>214</sup>

Despite significantly updating the authorization process for cyber operations in the White House, NSPM-13 was highly classified, and the White House refused to share the document with any member of Congress.<sup>215</sup> In a letter to President Trump in February 2019, a bipartisan group of HASC members expressed concern over the withholding of NSPM-13.<sup>216</sup> Noting that “it is unacceptable that the White House continues to stonewall [Congress’s] attempts to oversee sensitive operations,” Representative Langevin introduced an amendment to the FY 2020 NDAA that would have required disclosure of NSPM-13.<sup>217</sup> While the amendment ultimately did not pass, Congress enacted a provision in the FY 2020 NDAA requiring

212. U.S. DEP’T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 2018 1 (2018).

213. See 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> [https://perma.cc/WA3A-KF4R].

214. See Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019, 8:22 AM), [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](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) [https://perma.cc/5D6H-9UCN].

215. Mark Pomerleau, *After Tug-of-War, White House Shows Cyber Memo to Congress*, FIFTH DOMAIN (Mar. 13, 2020), <https://www.fifthdomain.com/congress/2020/03/13/after-tug-of-war-white-house-shows-cyber-memo-to-congress> [https://perma.cc/YA5C-M4AV].

216. Letter from the H. Comm. on Armed Servs. to Donald J. Trump, President of the United States (Feb. 28, 2019), [https://s.wsj.net/public/resources/documents/cyber0710.pdf?mod=article\\_inline](https://s.wsj.net/public/resources/documents/cyber0710.pdf?mod=article_inline) [https://perma.cc/2VFG-V7B9].

217. See Press Release, Rep. Jim Langevin (D-RI), House of Representatives, Langevin Statement on Trump Administration’s Refusal to Provide Congress with Cyberspace Operations Directive (July 10, 2019), <https://langevin.house.gov/press-release/langevin-statement-trump-administrations-refusal-provide-congress-cyberspace> [https://perma.cc/6WZZ-YLHQ].

the Secretary of Defense to notify HASC and SASC of any delegation of authority from the National Command Authority, including operational details,<sup>218</sup> to ensure transparency over where cyber authorities reside.<sup>219</sup> Only in March 2020 did the White House share NSPM-13 with Congress,<sup>220</sup> although the document remains inaccessible to members who have not received the necessary security clearance.<sup>221</sup>

The Trump administration's secrecy prompted concerns that the DOD was increasingly keeping Congress in the dark about its cyber operations.<sup>222</sup> Under the new authorities granted to it in 2018, according to some reports, Cyber Command "conducted many more operations."<sup>223</sup> For example, in June 2019, during a period of escalating incidents with Iran that included the downing of an American drone, the United States conducted an offensive cyber operation against an Iranian intelligence group in lieu of a military strike.<sup>224</sup> In the FY 2020 NDAA, Congress updated the sensitive military cyber operations notification requirement to bolster oversight, providing more specificity on operations that are "sensitive" and must be reported.<sup>225</sup> The HASC report noted that "the Department's definition of and threshold for sensitive military cyber operations is not aligned with the intent of the committee" and expressed its expectation "to be continually notified and kept fully and currently informed," suggesting that HASC was dissatisfied with the frequency and lack of detail of the DOD's reports.<sup>226</sup> Accordingly, the FY 2020 NDAA added a series of specific risk thresholds and triggers for notification, including a medium to high risk of collateral

---

218. FY 2020 NDAA, *supra* note 182, § 1642(a)(1).

219. Interview with Department of Defense Lawyer, *supra* note 196.

220. Pomerleau, *supra* note 215.

221. See *National Security Presidential Memoranda [NSPMs], Donald J. Trump Administration*, FED'N OF AM. SCIENTISTS, <https://fas.org/irp/offdocs/nspm/index.html> [<https://perma.cc/KF4Q-WVAS>] (listing NSPM-13, but not providing a public link).

222. See Volz, *supra* note 213.

223. 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> [<https://perma.cc/MBU5-MFMT>].

224. Julian E. Barnes & Thomas Gibbons-Neff, *U.S. Carried Out Cyberattacks on Iran*, N.Y. TIMES (June 22, 2019), <https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html> [<https://perma.cc/M8C9-78Z2>].

225. See FY 2020 NDAA, *supra* note 182, § 1632.

226. H.R. REP. NO. 116-120, at 300 (2019).

effects (estimated or actual), intelligence gain or loss, probability of retaliation, or probability of unintended detection.<sup>227</sup> Although these parameters were intended to facilitate greater compliance with the statute, Chesney has pointed out that there was “some play in the joints when it comes to distinguishing low from medium risk,” and that thresholds could “be construed too broadly in some cases” to frustrate oversight.<sup>228</sup> Similarly, the FY 2020 NDAA also required the DOD to submit to HASC and SASC a written annual report “summarizing all named military cyber operations,” including both “cyber effects[ ] operations” and “cyber effects enabling operations,” although the NDAA and its legislative history fail to define these key terms.<sup>229</sup> In the following year, the FY 2021 NDAA added a few more reporting requirements to the quarterly cyber operations briefings. With congressional frustration mounting about the DOD’s failure to keep it apprised, SASC reiterated that the briefings should include “all offensive and significant defensive military operations” and reporting of operations “even short of effects.”<sup>230</sup>

The FY 2021 NDAA also updated the sensitive military cyber operations notification statute, changing the definition of “sensitive military cyber operations” from a focus on geographic location to the identity of the targets.<sup>231</sup> Rather than requiring notification of operations outside an area of hostilities, the statute now defines sensitive military cyber operations as those that are “intended to achieve a cyber effect against a foreign terrorist organization or a country, including its armed forces and the proxy forces of that country located elsewhere” with which the United States is not involved in hostilities or has not acknowledged being involved in hostilities.<sup>232</sup> Although it is not clear what specifically prompted the

227. FY 2020 NDAA, *supra* note 182, § 1632.

228. 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> [<https://perma.cc/WN45-HVH8>].

229. FY 2020 NDAA, *supra* note 182, § 1644(a). For the reporting requirements, see Appendix A: Cyber Operations, *supra* note 173.

230. S. REP. NO. 116-236, at 337 (2020).

231. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1702, 134 Stat. 3388, 4080-81 (2020) (codified as amended at 10 U.S.C. § 395) [hereinafter FY 2021 NDAA].

232. *Id.*

modification,<sup>233</sup> the revised provision means that the defense committees must now be notified when cyber operations target new adversaries. For example, the defense committees would not be notified of cyber operations against the Assad regime under the old definition, since the United States is already engaged in hostilities in Syria, even if not against the regime. However, the same operation would have to be reported under the new definition.

Finally, Congress directed the DOD to take additional steps to define a framework for cyber operations, with the goal of ensuring their effectiveness.<sup>234</sup> Section 1720 of the FY 2021 NDAA required the Secretary of Defense to develop a framework to enhance the “consistency, execution, and effectiveness of cyber hunt forward operations.”<sup>235</sup> The framework includes many requirements, including identifying selection criteria for proposed operations and metrics to evaluate their effectiveness, and mandating a briefing to the defense committees by May 1, 2021.<sup>236</sup> In its committee report, SASC endorsed the DOD’s hunt forward operations and explained that the framework would “institutionaliz[e] these missions within the Department” and enable the “execution of more successful missions at an increased operational tempo.”<sup>237</sup>

---

233. Robert Chesney’s take is that the provision:

remove[s] that geographic test altogether (thus moving away from an apparent focus on flagging cases entailing risk of diplomatic repercussions), replacing it with ... a test triggered only where the targeted adversary is “a foreign terrorist organization or country” (including a govt’s proxies) “with which” American forces “are not involved in hostilities” (reflecting concern w/mission creep/expansion & escalation risk) ... In short: high-stakes military cyber ops against FTOs and government-controlled entities would all be subject to notification, wherever they play out, except when we are in hostilities with that adversary already.

Bobby Chesney (@BobbyChesney), TWITTER (Dec. 3, 2020, 11:00 PM), <https://twitter.com/bobbychesney/status/1334709170239664130?s=11> [<https://perma.cc/TJP4-NR96>].

234. FY 2021 NDAA, *supra* note 231, § 1720.

235. *Id.* § 1720(a).

236. *Id.* § 1720(b)-(c).

237. S. REP. NO. 116-236, at 336 (2020).

Table 2: Summary of Cyber Operations Oversight Provisions<sup>238</sup>

Cyber Operations Reporting & Notification Requirements		
Provision	Requirement	Recipient
Various	One-time reports on DOD’s cyber warfare policy.	HASC; SASC
10 U.S.C. § 484 (FY 2014 NDAA)	“[Q]uarterly briefings on all offensive and significant defensive military operations in cyberspace” during the preceding quarter.	HASC; SASC
10 U.S.C. § 395 (FY 2018 NDAA)	48-hour notification of “any sensitive military cyber operation conducted under this title.”	HASC; SASC
10 U.S.C. § 396 (FY 2018 NDAA)	Quarterly reporting of cyber weapons reviews; 48-hour notification of the use of cyber weapons.	HASC; SASC
FY 2018 NDAA, § 1644, <i>amended by</i> FY 2020 NDAA, § 1635	Quadrennial review of the “cyber posture of the United States.”	HASC; SASC
FY 2019 NDAA, § 1642(a)	Quarterly reporting of actions undertaken by Cyber Command pursuant to the authorization “to take appropriate and proportional action in foreign cyberspace” in response to an “active, systematic, and ongoing campaign of attacks” by Russia, China, North Korea, or Iran.	HASC; SASC
FY 2019 NDAA, § 1642(c)	Annual report on “the scope and intensity” of information operations and cyber attacks by Russia, China, North Korea, and Iran against the United States and “adjustments of the Department of Defense in the response directed or recommended by the Secretary.”	HASC; SASC HFAC; SFRC HPSCI; SSCI

238. All provisions in Figure 2 also require reporting to the House and Senate appropriations committees.

FY 2020 NDAA, § 1644	Annual report “summarizing all named military cyberspace operations conducted in the previous calendar year.”	HASC; SASC
-------------------------	---	------------

In sum, in recent years, Congress has strongly supported and encouraged more proactive use of cyber operations in countering malicious actors. To fill oversight gaps over these new operations, which fell at the intersection of military and intelligence operations, Congress created new oversight obligations. But in solving one problem, it created another: the NDAA process led by the armed services committees resulted in the consolidation of military cyber oversight in the hands of only one subset of Congress—the armed services committees. It left little to no role for the foreign relations or intelligence committees, despite the fact that foreign relations and intelligence concerns are very much present when Cyber Command undertakes computer network operations against a target outside an ongoing warzone. The novel oversight and legal challenges presented by military cyber operations offered an opportunity for congressional committees to think holistically about oversight, but instead, HASC and SASC built on and reinforced existing committee silos.

### III. THE PATHOLOGY OF MODERN WARFARE OVERSIGHT: INFORMATION SILOING

The most significant and consequential challenge presented by Congress’s efforts to respond to the challenges of modern warfare as described in Part II is that it has entrenched a system in which information and reporting is segmented between discrete congressional committees. The structural challenge impedes effective, cohesive oversight over modern warfare. Information known to members of one committee may be relevant to the work of another but may nonetheless not be shared with that committee’s members. Legislators are thus left to make decisions on crucial national security matters without access to the full range of relevant information. This disjointed system likewise harms the executive branch, which could be subject to poorly informed and ill-advised oversight. As long

as this problem remains unsolved, Congress will find itself increasingly incapable of effectively exercising its constitutional role in overseeing the executive branch's conduct of modern warfare.

### *A. Information Siloing: A Problem of Congress's Own Making*

As Part II described, nearly every year since 2013, Congress has strengthened and clarified modern warfare oversight measures.<sup>239</sup> Due to significant challenges with passing legislation,<sup>240</sup> nearly all of these requirements have been included in the “must pass” annual NDAA.<sup>241</sup> Because the NDAA is “the only piece of legislation getting through on an annual basis, it becomes a Christmas tree on which everything else is hung,” a congressional staff member explained.<sup>242</sup> The NDAA process is under the armed services committees' jurisdiction, giving these committees authorizing power over the bill.<sup>243</sup>

#### *1. The Power of the “Must Pass” NDAA*

The armed services committees have leveraged their privileged position in the NDAA process to consolidate their jurisdiction over

239. See *supra* Part II.

240. The average number of laws passed each year has declined considerably over the past decades. Three hundred forty-four laws were passed from January 2019 to January 2021, compared to 736 laws passed from January 1979 to December 1980. *Statistics and Historical Comparison*, GOVTRACK, <https://www.govtrack.us/congress/bills/statistics> [<https://perma.cc/35Y2-DU8X>]; see also *Vital Statistics on Congress, Chapter 6: Legislative Productivity in Congress and Workload*, BROOKINGS INST. (Feb. 8, 2021), <https://www.brookings.edu/multi-chapter-report/vital-statistics-on-congress> [<https://perma.cc/56XV-2B6F>]. For analysis on the reasons for this productivity decline, see Derek Willis & Paul Kane, *How Congress Stopped Working*, PROPUBLICA (Nov. 5, 2018, 10:00 AM), <https://www.propublica.org/article/how-congress-stopped-working> [<https://perma.cc/DGN4-QJLZ>]; Ella Nilsen, *House Democrats Have Passed Nearly 400 Bills. Trump and Republicans Are Ignoring Them*, VOX (Nov. 29, 2019, 7:00 AM), <https://www.vox.com/2019/11/29/20977735/how-many-bills-passed-house-democrats-trump> [<https://perma.cc/NU8Q-T4AS>]; Jesse M. Crosson, Alexander C. Furnas, Timothy Lapira & Casey Burgat, *Partisan Competition and the Decline in Legislative Capacity Among Congressional Offices*, LEGIS. STUD. Q., July 2019, at 1.

241. See Amanda Chuzi, *Can Congress' “Most Successful Bill” Fix the Legislative Branch?*, WAR ON THE ROCKS (June 5, 2020), <https://warontherocks.com/2020/06/can-congress-most-successful-bill-fix-the-legislative-branch> [<https://perma.cc/5PXT-VEYM>].

242. Interview with Congressional Staff Member #2, *supra* note 175.

243. VALERIE HEITSHUSEN & BRENDAN W. MCGARRY, CONG. RSCH. SERV., IF10515, DEFENSE PRIMER: THE NDAA PROCESS (2021).

modern warfare operations—whether it is drones, special operations, security cooperation, or cyber.<sup>244</sup> This reporting scheme tracks the fact that the DOD implements most counterterrorism and cyber operations, and the armed services committees have jurisdiction over most DOD operations. But as discussed in Part II, the statutory oversight framework has explicitly excluded other relevant committees from even being made aware of the reporting, despite those committees' clear equities in modern warfare operations.<sup>245</sup> Likewise, the intelligence committees keep intelligence reporting extremely closely held, pointing to the highly classified nature of the information to avoid informing other committees. Thus, each of the three respective sets of committees—armed services, intelligence, and foreign relations—have their own discrete reporting pipeline, which has led to information silos and knowledge gaps that frustrate comprehensive oversight.<sup>246</sup>

## 2. Committee Membership Rules

Political party rules have further complicated this siloing problem by prohibiting joint membership between related committees. For example, Republican senators are prohibited from serving on both SASC and SFRC.<sup>247</sup> There have been some attempts to overcome the problem and facilitate information flow by requiring that certain members serve on multiple related committees. In the House of Representatives, for instance, at least one Democratic

---

244. For the full chart, see Appendix A: Cyber Operations, *supra* note 173; Oona A. Hathaway, Tobias Kuehne, Randi Michel & Nicole Ng, Appendix B: Special Operations, Drone Strikes, and Targeted Killings (same URL) [hereinafter Appendix B: Special Operations, Drone Strikes, and Targeted Killings]; Oona A. Hathaway, Tobias Kuehne, Randi Michel & Nicole Ng, Appendix C: Security Cooperation (same URL) [hereinafter Appendix C: Security Cooperation].

245. See *supra* Part II; see also Appendix A: Cyber Operations, *supra* note 173; Appendix B: Special Operations, Drone Strikes, and Targeted Killings, *supra* note 244; Appendix C: Security Cooperation; *supra* note 244.

246. In fact, cybersecurity oversight more generally is spread across multiple committees, including armed services, intelligence, homeland security, and commerce, among others, but information is not always shared between committees. As one committee staffer described, “[e]very committee on the Hill has a piece of cyber,” resulting in a “very convoluted picture.” Interview with Congressional Staff Member #3, *supra* note 19.

247. As well as judiciary and appropriations. JUDY SCHNEIDER, CONG. RSCH. SERV., 98-183, SENATE COMMITTEES: CATEGORIES AND RULES FOR COMMITTEE ASSIGNMENTS 1 (2014).

member must serve on both HFAC and HASC.<sup>248</sup> Nevertheless, a congressional staff member observed that only having one or two joint members (all below the leadership level) has minimal impact on cross-committee information sharing since the committee chairs and ranking members remain uninformed and it is challenging for one member to significantly steer the conversation.<sup>249</sup>

### 3. Classification Restrictions

Even when some members sit on multiple committees, they are often restricted from sharing information due to classification rules, even if directly relevant to matters before the committee. Although members of Congress are entitled to access classified information by virtue of their offices, their staff are generally not.<sup>250</sup> Members of Congress also are not automatically entitled to “Sensitive Compartmented Information” (SCI) access.<sup>251</sup> Some, though not all, classified information is separated into “compartments.”<sup>252</sup> These compartments are independent of the classification level. There can be compartmented information at every level of classification, and only those with access to the particular compartment can access the information, even if they otherwise have

---

248. Both Representatives Bill Keating and Chrissy Houlahan currently serve on the House Foreign Affairs and Armed Services Committees. *Committees and Caucuses*, OFF. OF CONGRESSMAN BILL KEATING, <https://keating.house.gov/policy-work/committees-and-caucuses> [<https://perma.cc/WQD9-MPYJ>]; *Committees and Caucuses*, OFF. OF CONGRESSWOMAN CHRISSY HOULAHAN, <https://houlahan.house.gov/about/committees-and-caucuses.htm> [<https://perma.cc/3S3D-VPMP>]. Joaquin Castro serves on both Foreign Affairs and Intelligence, and Jackie Speier serves on both Armed Services and Intelligence. *Committees and Caucuses*, OFF. OF CONGRESSMAN JOAQUIN CASTRO, <https://castro.house.gov/about/committees-and-caucuses> [<https://perma.cc/SE57-ZNET>]; *Committees*, OFF. OF CONGRESSWOMAN JACKIE SPEIER, <https://speier.house.gov/committees> [<https://perma.cc/EVY9-8Q67>].

249. Interview with Congressional Staff Member #1 (Aug. 26, 2020).

250. See 50 U.S.C. § 3163 (exempting members of Congress, but not their staff, from statutory provisions governing access to classified information); Mandy Smithberger & Daniel Schuman, *A Primer on Congressional Staff Clearances*, POGO (Feb. 7, 2020), <https://www.pogo.org/report/2020/02/a-primer-on-congressional-staff-clearances> [<https://perma.cc/M3MS-RJ9U>]; FREDERICK M. KAISER, CONG. RSCH. SERV., RS20748, PROTECTION OF CLASSIFIED INFORMATION BY CONGRESS: PRACTICES AND PROPOSALS 1, 3 (2011); MICHELLE D. CHRISTENSEN, CONG. RSCH. SERV., R43216, SECURITY CLEARANCE PROCESS: ANSWERS TO FREQUENTLY ASKED QUESTIONS 4, 5 (2016).

251. See Smithberger & Schuman, *supra* note 250.

252. See *id.*

the appropriate level of security clearance (for example, Top Secret (TS)). Who decides who has access to particular compartments? Access is granted on a “need to know” basis.<sup>253</sup> So who decides who needs to know? Congress and the executive branch differ on that. Congress maintains that it has the right to make the determination, but the executive branch maintains that the decision “is made by the agency where the information originated.”<sup>254</sup>

In the face of this standoff, the executive branch, which controls access to the information, wins. A former senior congressional staffer expressed that if Congress were to assert its authority to make rules about access to classified information, the executive branch might be more willing to work with Congress.<sup>255</sup>

In any case, the consequences of members’ inability to share information across committees can be serious. For instance, on January 2, 2020, a U.S. drone strike killed Major General Qassim Soleimani, the commander of Iran’s Islamic Revolutionary Guard Corps Quds Force, without consultation or approval from Congress.<sup>256</sup> The strike capped off over a year of escalation between the United States and Iran that brought both countries to the brink of war.<sup>257</sup> Following the Soleimani strike, SASC and SFRC debated possible strategic responses but lacked crucial information about

---

253. For more on the “need to know” and other requirements for Special Compartmented Information (SCI) access, see U.S. DEP’T OF DEF., DEPARTMENT OF DEFENSE MANUAL NO. 5105.21-V3, SENSITIVE COMPARTMENTED INFORMATION (SCI) ADMINISTRATIVE SECURITY MANUAL 11-14 (2020), [https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/510521m\\_vol3.pdf?ver=2020-09-15-132603-533](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/510521m_vol3.pdf?ver=2020-09-15-132603-533) [<https://perma.cc/2H6Z-KFD3>].

254. Smithberger & Schuman, *supra* note 250.

255. Interview with Jamil N. Jaffer, *supra* note 27.

256. Mustafa Salim, Missy Ryan, Liz Sly & John Hudson, *In Major Escalation, American Strike Kills Top Iranian Commander in Baghdad*, WASH. POST (Jan. 3, 2020, 3:02 AM), [https://www.washingtonpost.com/world/national-security/defense-secretary-says-iran-and-its-proxies-may-be-planning-fresh-attacks-on-us-personnel-in-iraq/2020/01/02/53b63f00-2d89-11ea-bcb3-ac6482c4a92f\\_story.html](https://www.washingtonpost.com/world/national-security/defense-secretary-says-iran-and-its-proxies-may-be-planning-fresh-attacks-on-us-personnel-in-iraq/2020/01/02/53b63f00-2d89-11ea-bcb3-ac6482c4a92f_story.html) [<https://perma.cc/8AHT-H6SM>]; Manu Raju & Ted Barrett, *Top Democratic Leaders Kept in Dark About Soleimani Attack*, CNN (Jan. 3, 2020, 2:46 PM), <https://www.cnn.com/2020/01/03/politics/congress-soleimani-attack/index.html> [<https://perma.cc/9EW2-J3X8>].

257. See Salim et al., *supra* note 256; Karoun Demirjian, *Senate Passes Resolution to Limit Trump’s Power to Order Military Action Against Iran*, WASH. POST (Feb. 13, 2020, 6:01 PM), [https://www.washingtonpost.com/national-security/senate-passes-resolution-limiting-trump-against-iran-in-bipartisan-vote/2020/02/13/d2f7429c-4e8f-11ea-bf44-f5043eb3918a\\_story.html](https://www.washingtonpost.com/national-security/senate-passes-resolution-limiting-trump-against-iran-in-bipartisan-vote/2020/02/13/d2f7429c-4e8f-11ea-bf44-f5043eb3918a_story.html) [<https://perma.cc/D92M-2D9Z>].

U.S. cyber operations against Iran.<sup>258</sup> Indeed, Senator Tim Kaine, a member of both SASC and SFRC, expressed frustration that he could not disclose information that was critical to SFRC's discussion of the Soleimani strike, but had been communicated to him in classified SASC briefings.<sup>259</sup> Most likely, this information was compartmented, and the relevant agency had determined that it was relevant to one committee (due to reporting requirements) but not the other. Senator Kaine also likely signed a nondisclosure agreement when he gained access to the compartmented information that prohibited him from disclosing anything he learned by virtue of that access.<sup>260</sup>

One committee staff member explained that the narrow compartmentalization of classified information has led to "frustrations even within the context of our committee," as information is limited to only certain members and staffers.<sup>261</sup> It can even create divisions between members and their staff. One staffer we spoke with recalled that he had relevant information from a previous committee assignment that he could not share with his boss, a member of Congress, because that member was not cleared into the relevant program. He could not even explain that there was information that the member needed to know without violating his nondisclosure obligations.<sup>262</sup>

Some observers argue that limiting information sharing is necessary to minimize the risk of unauthorized disclosures and that even the perception of potential leaks resulting from extensive disclosure may dissuade an agency from sharing operational details or from briefing Congress at all.<sup>263</sup> As one former congressional staff member explained, "Congress always gets tarnished with its reputation as being leakers."<sup>264</sup> However, the interviewee argued, this concern is vastly overblown, as the few members of Congress known

258. Interview with Congressional Staff Member #1, *supra* note 249.

259. *Id.*

260. It is possible that he considered himself bound by the "secrecy oath" that some members and staff are required by Senate rules to take. See KAISER, *supra* note 84, at 4.

261. Interview with Congressional Staff Member #3, *supra* note 19.

262. Interview with Jamil N. Jaffer, *supra* note 27.

263. Heidi Kitrosser, *Congressional Oversight of National Security Activities: Improving Information Funnels*, 29 CARDOZO L. REV. 1049, 1071 (2008).

264. Interview with former Congressional Staff Member #6, *supra* note 7.

for leaking are not typically on committees with jurisdiction over national security matters.<sup>265</sup> Of course, observers disagree as to the magnitude of the leakage problem and whether the executive branch over-classifies information, creating more problems than it solves.<sup>266</sup> In addition, the executive branch at times simply fails to specify exactly what information is classified. One congressional staffer observed, “Generally members walk out of intelligence briefings and they don’t know what is and isn’t classified. Because the DNI uttered the words they feel like they can’t say anything, even though details were reported by the New York Times.”<sup>267</sup>

Classification also restricts the potential for informal relationship-based information sharing. The siloing of reporting streams would be significantly less consequential if committees had a formal or even informal mechanism to exchange information. Classification restrictions, however, inhibit committee members and staffers from ensuring their colleagues with equities in the matter are informed.

#### 4. *Inter-Committee Turf Wars*

This siloing dynamic reflects and is exacerbated by a more fundamental challenge within Congress: enduring turf wars between committees.<sup>268</sup> In a world where “information is power,” congressional committees have incentives to keep information closely held.<sup>269</sup> Former Director for Counterterrorism at the National Security Council (NSC) Daniel Rosenthal explains that “the oversight committees often compete with one another for access to information

---

265. *Id.*

266. For more information on over-classification by the executive branch, see April Doss, *The White House Abused the Classification System*, ATLANTIC (Oct. 8, 2019), <https://www.theatlantic.com/ideas/archive/2019/10/uses-and-abuses-information-classification/599533> [<https://perma.cc/MB93-ZR6G>]; *Examining the Costs of Overclassification on Transparency and Security: Hearing Before the H. Comm. on Oversight and Gov’t Reform*, 114th Cong. 2 (2016) (statement of Rep. Jason Chaffetz, Chairman, H. Comm. on Oversight and Gov’t Reform) (“Estimates range from 50 to 90 percent of classified material is not properly labeled.”); Ann Koppuzha, *Secrets and Security: Overclassification and Civil Liberty in Administrative National Security Decisions*, 80 ALB. L. REV. 501, 507-09 (2016); Oona A. Hathaway, *Secrecy’s End*, 107 MINN. L. REV. (forthcoming 2021).

267. Interview with Congressional Staff Member #4, *supra* note 59.

268. See generally DAVID C. KING, *TURF WARS: HOW CONGRESSIONAL COMMITTEES CLAIM JURISDICTION* 11-12 (1997).

269. Interview with Congressional Staff Member #3, *supra* note 19.

and actively lobby the executive branch to deny the other oversight committees access to information that they deem within their sole jurisdiction.”<sup>270</sup> Without a forcing mechanism like the executive branch’s NSC-led interagency policy process, committees “jealously guard their territories.”<sup>271</sup> A congressional staffer observed that “the deployment of cyber tools is one of the most closely guarded secrets.”<sup>272</sup> Turf wars are also reinforced by a committee’s sense of its own culture and traditions. Despite the foreign relations committees’ jurisdiction over war powers, the sense of the armed services committees is that they are the committees that really “do war.”<sup>273</sup>

Committees lack the incentives to share information, and leadership and personalities can entrench the turf war mindset. One congressional staffer remarked that the absence of information access creates more curiosity than is warranted.<sup>274</sup> Yet, when a committee does let down its guard and allows outside members to gain access to its information, there is always a “risk that insight turns into oversight.”<sup>275</sup> According to interviews with congressional staff members, a committee’s ability to assert its jurisdiction and guard information also depends on the personalities of committee and congressional leadership. For example, Speaker of the House Nancy Pelosi, as a former HPSCI member, has, according to one interviewee, supported the intelligence committees’ efforts to withhold information from other committees. Likewise, committee leaders’ specific personalities, stature, and assertiveness can significantly influence the committee’s success in jurisdictional turf battles.<sup>276</sup>

This Section has examined how Congress itself has contributed to information siloing among committees operating in the national security context. The next Section shows how this development has undermined Congress’s capacity to effectively oversee the work of the executive branch in the national security arena.

270. Daniel Rosenthal, “*Congress Perhaps?*” *Congressional Oversight and the U.S. Drone Program*, CTR. FORA NEWAM. SEC. (July 31, 2018), <https://www.cnas.org/publications/reports/congress-perhaps-congressional-oversight-and-the-u-s-drone-program> [<https://perma.cc/B2K2-HP43>].

271. Interview with Congressional Staff Member #1, *supra* note 249.

272. Interview with Congressional Staff Member #4, *supra* note 59.

273. Interview with Jamil N. Jaffer, *supra* note 27.

274. Interview with Congressional Staff Member #5, *supra* note 22.

275. *Id.*

276. See Interview with Congressional Staff Member #4, *supra* note 59.

*B. Siloing and Its Implications for Oversight and National Security*

While committees may gain political benefits from guarding their turfs, information siloing frustrates Congress's ability to carry out effective oversight of the executive branch. The information gaps resulting from siloing of reporting and notification may lead to poorly informed and under-vetted congressional decision-making. Ultimately, information siloing of modern military operations can harm national security and foreign relations.

*1. Siloing Obstructs Deliberation and Informed Legislating*

Information siloing can obstruct deliberation and thus block informed legislating. If an operation is briefed to only one committee, members who are informed may lack the ability to engage in meaningful deliberation with other members, thereby impeding a proper response.<sup>277</sup> A former SFRC staffer expressed the difficulty of conducting effective oversight when the committee is left in the dark on related operations: “[H]ow can you make foreign relations policy without having access to one of the most potentially influential capabilities to influence foreign relations?”<sup>278</sup> Another staffer illustrated the dilemma with a hypothetical: imagine there is a critical intelligence program that involves close cooperation with the military of a partner country.<sup>279</sup> The foreign relations committees have not been briefed on, and are not aware of, the program. As a result, they may not understand why the administration refuses to press that country on its human rights record—a record that “we would never let go generally.”<sup>280</sup> If the foreign relations committees do not know about the intelligence program, they would be unable to understand why U.S. foreign policy toward that country contradicts our values. And they would not be in a position to discuss the appropriateness of this foreign policy trade-off.<sup>281</sup> When issues are

---

277. See KAISER, *supra* note 84, at 5-6.

278. Interview with Jamil N. Jaffer, *supra* note 27.

279. Interview with former Congressional Staff Member #6, *supra* note 7.

280. *Id.*

281. *Id.*

briefed just to the Gang of Eight, the problems of impeded information sharing become particularly acute. As a former staffer explained, “Then it’s just a small group of members. It causes all kinds of spillover effects.”<sup>282</sup> For instance, when Congress was asked to reauthorize the § 215 collection program in 2011, most members were unaware of existing bulk collection programs carried out under intelligence authorities.<sup>283</sup> Committee members had to fight to get a document describing these activities opened up to members, and then only in a Sensitive Compartmented Information Facility (SCIF) at the TS/SCI level.<sup>284</sup> If that had not been done, members voting on the reauthorization would have been entirely unaware of how it interacted with existing collection programs.<sup>285</sup>

Indeed, to exercise their authorities over the process of commencing war via authorizations for the use of force or restricting uses of force through the WPR, the foreign relations committees must be fully informed of uses of U.S. military power. After the Soleimani strike, for example, the foreign relations committees weighed what might be an appropriate response to Iranian retaliation, while being left in the dark about the ongoing or potential cyber, intelligence, and other operations between the United States and Iran.<sup>286</sup> While the Senate and House ultimately voted to restrain the President from using force, better information sharing would have allowed the senators to make a more informed decision.<sup>287</sup>

Information siloing poses a particularly acute challenge to deliberation and informed legislating on cross-jurisdictional issues like cyber operations. As a DOD lawyer observed, congressional committees “are not structured to take a holistic approach to the problem of cyberspace,” which challenges traditional paradigms of jurisdiction that are focused on physical spaces (for example, commercial, domestic, and overseas) and actors (for example, government agencies, departments, and private sector).<sup>288</sup> Cyber operations and cybersecurity transcend these distinctions and cut

282. Interview with Jamil N. Jaffer, *supra* note 27.

283. *Id.*

284. *Id.*

285. *Id.*

286. See *supra* notes 256-58 and accompanying text.

287. Demirjian, *supra* note 257; Wise, *supra* note 70.

288. Interview with U.S. Department of Defense Lawyer, *supra* note 196.

across issues of foreign affairs, intelligence, and defense, but congressional committees remain confined by these parameters. The Cyberspace Solarium Commission observed that the dispersal of oversight responsibilities across numerous committees and subcommittees “prevents Congress from effectively providing strategic oversight of the executive branch’s cybersecurity efforts or exerting its traditional oversight authority for executive action and policy in cyberspace.”<sup>289</sup> Information siloing also complicates oversight over military cyber operations, which blur the jurisdictional lines between Title 10 and Title 50 that traditionally divided military and intelligence oversight within Congress.<sup>290</sup> As Tressa Guenov and Tommy Ross have observed, “It is nearly impossible to consider cyber deterrence and the role of offensive cyber attacks in military operations without encroaching on business, homeland security, foreign policy, and criminal justice issues.”<sup>291</sup>

Information siloing also limits the ability of committees to consider how various legislative actions might affect and be affected by other programs already in place. Consider a hypothetical example involving Russia. In weighing whether and how to craft sanctions legislation against Russia for election interference, the foreign relations committees should have an understanding of all the tools brought to bear against Russia to counter or deter meddling—including cyber operations, such as those carried out by Cyber Command during the 2018 midterm elections.<sup>292</sup> More generally, as relations with Russia remain tense, since the foreign relations committees are charged with overseeing the executive’s conduct of foreign relations with Russia,<sup>293</sup> it is critical that they understand the full nature of the bilateral relationship, including hostile and potentially escalatory activities like military cyber operations. However, although there may be informal exchanges of

---

289. U.S. CYBERSPACE SOLARIUM COMM’N, *supra* note 20, at 35.

290. *See supra* Part II.A.

291. Tressa Guenov & Tommy Ross, *At A Crossroads, Part I: How Congress Can Find Its Way Back to Effective Defense Oversight*, WAR ON THE ROCKS (Mar. 9, 2018), <https://warontherocks.com/2018/03/at-a-crossroads-part-i-how-congress-can-find-its-way-back-to-effective-defense-oversight> [<https://perma.cc/5XW8-QCP7>].

292. *See* Pomerleau, *supra* note 223. We are not aware of whether this operation was reported to the armed services committees as a sensitive military cyber operation, nor do we know whether the foreign relations committees were informed of the operation.

293. *See* SFRC BACKGROUND, *supra* note 34, at 4.

information, the DOD is under no statutory obligation to report cyber operations against Russia to the foreign relations committees.<sup>294</sup>

The foreign relations committees are particularly affected by their lack of access to information about other programs and operations. While successive iterations of the NDAA have established new reporting and notification requirements for modern military operations, the reports almost all go to the armed services committees. The foreign relations committees receive virtually none of that information. This is even the case for operations with implications falling squarely within the foreign relations committees' jurisdiction. One telling example is the aforementioned FY 2019 NDAA, which functions as a quasi-AUMF for cyber operations against Russia, China, North Korea, and Iran.<sup>295</sup> The consequences extend beyond the committees' role in use of force authorizations, as well. For example, as described earlier, when HFAC was considering a "massive Pakistan aid package," the CIA failed to inform the committee of the drone program in that country, even though it had obvious implications for U.S.-Pakistan relations.<sup>296</sup> HFAC chairman Howard Berman was ultimately informed about the drone program, but he could not share the information with the rest of the committee because he was the only member read into the highly classified program.<sup>297</sup> And in 2014, the SFRC considered and supported legislation to train and equip Syrian rebels, even though the chair and ranking member did not know any details of what media later reported to be the CIA's parallel covert program,<sup>298</sup> which had been initiated the year before.<sup>299</sup>

---

294. See Appendix A: Cyber Operations, *supra* note 173.

295. See *supra* notes 200-02 and accompanying text.

296. Interview with Congressional Staff Member #4, *supra* note 59.

297. *Id.*

298. Interview with Jamil N. Jaffer, *supra* note 27.

299. See Tom Bowman & Alice Fordham, *CIA Is Quietly Ramping up Aid to Syrian Rebels, Sources Say*, NPR (Apr. 23, 2014, 5:05 PM), <https://www.npr.org/sections/parallels/2014/04/23/306233248/cia-is-quietly-ramping-up-aid-to-syrian-rebels-sources-say> [<https://perma.cc/HX2V-U8LG>]; Mazzetti et al., *supra* note 131.

## 2. *Siloing Means No Committee Has the Complete Picture*

Information siloing means that no committee—and no member—has the complete picture of modern warfare operations. As a result, members are often called on to make crucial decisions without the full range of relevant information in hand. Based on our interviews, information siloing appears to be a particularly significant problem in the counterterrorism context, including special forces operations and drone strikes.<sup>300</sup> As former National Security Council Director for Counterterrorism Daniel Rosenthal explained:

[N]umerous members of Congress, countless congressional staffers, and multiple committees all have access to some information about the drone program.... [N]o single member of Congress, congressional staffer, or oversight committee has visibility over all drone platforms, all strikes, taken in all theaters both within and outside of areas of active hostilities.<sup>301</sup>

The tragic events in Niger that led to the deaths of American special forces, recounted at the outset of this Article, illustrate some of the dangers that can result from this lack of visibility. Those deaths might have been avoided if not for the siloed oversight over those operations, which meant that no one in Congress was aware of the full extent of U.S. involvement in the country. Even when there is the rare collaboration between committees, the foreign relations committees are often the odd man out. This is true even though counterterrorism operations generally require the approval of the U.S. embassy for the country where the operation will take place.<sup>302</sup> U.S. embassies and consulates are part of the State Department (organized under the Bureau of Consular Affairs)<sup>303</sup> and thus under the oversight jurisdiction of the foreign

---

300. A congressional staff member highlighted that the siloing problem affects both counterterrorism and cyber operations, but is more acute in the counterterrorism context. Interview with Congressional Staff Member #5, *supra* note 22.

301. Rosenthal, *supra* note 270.

302. Though their approval is necessary, ambassadors can be overridden. See SERAFINO, *supra* note 113, at 9.

303. See *About Us—Bureau of Consular Affairs*, U.S. DEP'T OF STATE, <https://www.state.gov/about-us-bureau-of-consular-affairs/> [<https://perma.cc/PS7G-DDDG>].

relations committees.<sup>304</sup> These committees are rarely notified of counterterrorism operations, despite the fact that they oversee embassies and diplomatic relations.<sup>305</sup> This information gap thus inhibits the committees' capacity to effectively oversee the agency for which they are responsible.

Information sharing restrictions and narrow notification and reporting obligations allow the executive branch to control committees' access to information. Like the foreign relations committees, the intelligence committees generally do not receive reporting or notification on military cyber operations. As one congressional staffer observed, "When it comes to DOD activities, HPSCI feels itself pretty frozen out."<sup>306</sup> The intelligence committees are only briefed on operations conducted under intelligence authorities. If Cyber Command and the CIA conduct coordinated or supported cyberattacks, each agency will brief its respective oversight committee on its own activities, and neither committee will have the full picture.<sup>307</sup> Moreover, it is often up to the executive to determine how much of a joint operation to disclose.<sup>308</sup>

Indeed, agencies sometimes exploit congressional committee jurisdictional divisions and turf wars to avoid onerous oversight. In the case of cyber operations, the armed services committees are perceived by some observers as friendlier to the military and less willing to engage in rigorous oversight.<sup>309</sup> The executive branch "will hand-feed the congressional committees that they care about, but they will do anything in their power to avoid cooperating with the 'other' committees."<sup>310</sup> As a former Cyber Command lawyer put it, "If you're the CIA you may say you aren't talking to the armed service committees, they do not have my interests at heart, and vice versa."<sup>311</sup> Information silos can thus privilege the executive branch at Congress's expense.

304. See *supra* Part I.A.

305. Interview with former Congressional Staff Member #6, *supra* note 7.

306. Interview with Congressional Staff Member #4, *supra* note 59.

307. See Rosenthal, *supra* note 270; Interview with Congressional Staff Member #5, *supra* note 22.

308. Interview with Congressional Staff Member #5, *supra* note 22.

309. Interview with Congressional Staff Member #1, *supra* note 249.

310. Rosenthal, *supra* note 270.

311. Interview with former Cyber Command Lawyer (Oct. 6, 2020).

### *3. Information Siloing Exacerbates Institutional Jealousies and Impedes Agency Coordination*

Information siloing may reinforce interagency competition within the executive branch, which may inhibit the government's broader capacity to effectively address security threats. Andru Wall explains that siloing is both "legally incongruous and operationally dangerous because it suggests statutory authorities are mutually exclusive and it creates concerns about interagency cooperation at exactly the time in history when our policy and legal structures should be encouraging increased interagency coordination and cooperation against interconnected national security threats."<sup>312</sup> In fact, when agencies compete with one another, they can leverage information silos to advance their own equities with their congressional patrons.

A former congressional staff member recalled an incident in which the CIA and the DOD sought to displace each other from parallel operations in the same country, which included efforts to elevate concerns up to the host country's head of state. "The oversight seams made this challenging," the staff member recalled, "on these committees, the agencies played members off each other, getting members to be advocates for them rather than overseers."<sup>313</sup> Members of Congress made calls to the White House on behalf of their agencies, asking why the other agency was involved. "This was embarrassing from an oversight standpoint, but also potentially damaging from a national security standpoint," the staffer added.<sup>314</sup>

\* \* \*

This Part has examined the ways in which information siloing impedes Congress's ability to provide effective oversight of modern warfare and thus harms national security. Ironically, while Congress publicly recognizes the challenges facing executive branch coordination and has urged stronger coordination,<sup>315</sup> it has not

---

312. Wall, *supra* note 11, at 92.

313. Interview with former Congressional Staff Member #6, *supra* note 7.

314. *Id.*

315. For example, in Avril Haines's January 19, 2021, confirmation hearing for her

applied the same logic or solutions to its own institutional structure. Siloing, therefore, does not merely cut out certain committees, but it also hinders Congress's ability to effectively carry out its legislating, war making, and oversight roles. The next Part considers possible reforms to address this problem.

#### IV. PROPOSALS FOR REFORM

When properly and effectively exercised, congressional oversight ensures that lawmakers have all the information they need to carry out their constitutional duties to monitor the activities of the executive branch and make appropriate legislative decisions. But the current regime falls short. As Part III demonstrated, Congress's approach to modern warfare oversight has entrenched information siloing, stymying Congress's ability to exercise rigorous and strategic oversight and leading to poorly informed and under-vetted congressional decision-making.<sup>316</sup> This Part first considers an ambitious structural reform to committee jurisdictions: the creation of a super committee to oversee all modern warfare operations. If the problem is that no committee has a complete view of the problem, the obvious solution is to join the committees together. But after considering how this might work, we conclude that the very same dynamics that have led to and entrenched information siloing would make such a solution impossible to implement and might even create other oversight problems. We then advance four alternative ambitious, but feasible, proposals to address information siloing. The most significant of these is the creation of a *Congressional National Security Council* to mirror the executive branch's National Security Council (NSC)—an institution created after World War II

---

nomination as Director of National Intelligence (DNI), Senator King asked Haines how she would "overcome ... the parochialism of the 11 agencies which you are called upon to lead?" He emphasized, "[D]on't forget the basic purpose [of the DNI position] was that we realized we had really good stovepipes, but they were still stovepipes. So, that's your mission." *On the Nomination of Avril D. Haines to be Director of National Intelligence: Hearing Before the S. Select Comm. on Intel.*, 117th Cong. 73-75 (2021) (statement of Sen. Angus King, Member, S. Select Comm. on Intel.), <https://www.intelligence.senate.gov/sites/default/files/hearings/t-ahaines-011921.pdf> [perma.cc/E9DV-DJKQ].

316. See *supra* Part III.A.

to address precisely the same problems on the executive branch side that Congress now faces.

*A. Why Not Create a Super Committee?*

The problems documented in this Article offer a strong argument in favor of significant structural reforms that would modify committee jurisdictions. If the problem is separate silos, after all, why not simply merge the silos into one? Perhaps the committees with equities in overseeing modern warfare—armed services, intelligence, and foreign relations—should be merged into a single committee, or at the very least they should receive the same reporting on cross-jurisdictional issues like counterterrorism and cyber operations.

This type of proposal is not new. The 9/11 Commission noted that there were seventeen congressional committees with some intelligence oversight duties and recommended better unifying congressional oversight to improve Congress's capacity to properly oversee intelligence activities.<sup>317</sup> Although the 9/11 Commission focused on a different problem, the challenges we document are similar: too many committees with responsibility for parts of the same problems and no committee with full insight into how these problems interrelate.

To be sure, creating a consolidated national security committee has advantages. First, there would be no more confusion between Title 10 and Title 50 reporting, no more information siloing or turf wars between these committees, and no duplicative briefings and multiplicitous reporting chains for the executive branch. Second, combining the committees would acknowledge the reality that separating Title 10 and Title 50 operations has become increasingly untenable in the post-9/11 world.<sup>318</sup> Third, having all the relevant reporting go to a single committee would reduce the potential for information gaps among lawmakers, allowing Congress to legislate more effectively.

Despite these potential advantages, the realities of Congress make merging committees difficult, if not outright impossible. Deep

---

317. 9/11 COMMISSION, *supra* note 108, at 103-07, 419.

318. *See supra* Part II.

structural change is hardly feasible unless there is extraordinary political will. Redrawing or eliminating committee jurisdictions will be met with intense opposition. As the 9/11 Commission put it, “Few things are more difficult to change in Washington than congressional committee jurisdiction and prerogatives.”<sup>319</sup> Siloing, after all, arises out of turf battles in which committees jealously guard their access to information. If a committee’s independence and separate existence are at stake, these turf battles will hardly give way. Replacing the armed services, foreign relations, and intelligence committees with a single national security committee is almost certainly impossible. More than one-quarter of the entire Senate is on SASC.<sup>320</sup> If the three committees were merged, the size of the merged committee would have to be smaller than the current size of the three combined, or it would be so large as to be incapable of functioning. But cutting members from these committees, each of which is considered a plum committee assignment, is politically fraught.

The alternative—creating a new “super committee” that would sit above the existing committees and address cross-jurisdictional issues—also faces functional and political challenges. If this new super committee gains jurisdiction, another committee will necessarily lose it. As one staff member put it, are the “members of armed services [going to] watch this super committee create really important legislation that’s partly in their jurisdiction and just let that go and not scream about it?”<sup>321</sup> In an environment where losing committee jurisdiction means losing the capacity to change key legislation, the answer is certainly no. The staff member added:

---

319. 9/11 COMMISSION, *supra* note 108, at 419. In fact, despite the 9/11 Commission’s emphatic call for structural reform, its recommendations were never implemented. See BIPARTISAN POL’Y CTR., TENTH ANNIVERSARY REPORT CARD: THE STATUS OF THE 9/11 COMMISSION RECOMMENDATIONS 16 (2011), <https://bipartisanpolicy.org/wp-content/uploads/2019/03/CommissionRecommendations.pdf> [<https://perma.cc/9Y6M-HCBZ>]. Seven years later, the Bipartisan Policy Center reflected that committee jurisdiction continued to be carved up to “accommodate antiquated committee structures,” as “[t]he rules governing congressional organization reflect the needs and economy of the 19th century, not the challenges of the 21st century.” *Id.*

320. *Committee Membership List: Committee on Armed Services*, U.S. SENATE, [https://www.senate.gov/general/committee\\_membership/committee\\_memberships\\_SSAS.htm](https://www.senate.gov/general/committee_membership/committee_memberships_SSAS.htm) [<https://perma.cc/7E9G-XSUP>] (listing twenty-six members).

321. Interview with Congressional Staff Member #5, *supra* note 22.

Nowadays we don't vote on amendments on the floor to influence a piece of legislation. That makes this [new super committee] structure harder. You vote for cloture or don't. You vote for the manager's packet of amendments or not. That's kind of how it works. If you aren't on the committee that produces the legislation, you don't get to play. The dysfunction that has settled in makes [a supercommittee] less realistic.<sup>322</sup>

Moreover, the expertise required for intelligence, military, and foreign affairs oversight differs considerably. Indeed, the intelligence committees were created as separate entities in the 1970s in part because it was understood that their members needed to specialize in the subject matter.<sup>323</sup> The merger would also raise challenges for agency oversight, as the committee would now be responsible for overseeing all the activities of the DOD *and* the CIA. Merging the committees would put seventeen intelligence agencies under the jurisdiction of the armed services and foreign relations/affairs committees, which would threaten to overburden committee members and staff and could result in less efficient, effective, and robust oversight overall.

A related structural fix—and one that might be more feasible—would be not to merge the committees themselves, but to merge the committees into a single committee only for cross-jurisdictional purposes, such as cyber-related reporting. Specifically, Congress could require that the armed services, intelligence, and foreign relations committees all receive the same reporting and notifications for cyber operations—such as forty-eight-hour notification of sensitive cyber military operations, quarterly briefings, and annual reports.<sup>324</sup> If every committee were to receive the same information, the argument goes, the siloing problem would significantly decrease, at least for the matters that are briefed.

Unfortunately, this proposal also runs into practical challenges. If each committee were to receive the same information, could any of them still be said to have jurisdiction over the issue? In Congress, jurisdiction is key. And with six committees receiving comprehensive reporting from the DOD, for example, all six might try to assert

---

322. *Id.*

323. See Johnson, *supra* note 200, at 199-201.

324. See Appendix A: Cyber Operations, *supra* note 173.

(sometimes conflicting) influence over the DOD. The armed services committees would almost certainly refuse to give up exclusive jurisdiction over certain military operations. Moreover, the DOD would likely vehemently resist this requirement, arguing that such a broad reporting regime would be too time-consuming and vulnerable to leaking. Instead, the DOD would likely listen to the committees that control its funding and appropriations: the defense committees.

A narrower version of this proposal would involve expanding the statutory recipients for only some of the reporting requirements to balance information sharing with jurisdictional concerns. In the context of cyber operations, reporting could be expanded for the quarterly cyber briefings, the annual report on named cyber operations, and the quadrennial cyber posture review.<sup>325</sup> However, the armed services committees may still resist losing their exclusive jurisdiction.<sup>326</sup> Proposals to expand reporting on cyber operations to the intelligence and foreign relations committees are also likely to run into the “slippery slope” problem, with critics arguing that other committees with some jurisdiction over cyber affairs, such as homeland security, commerce, and judiciary, will seek to be included as well.<sup>327</sup>

Notably, the widely celebrated Solarium Commission Report proposes a variation on the committee reorganization theme: it recommends that the House and Senate each create a select committee on cybersecurity to consolidate budgetary and legislative jurisdiction over cybersecurity issues.<sup>328</sup> The proposal, in addition to likely running into some of the practical impediments that any proposal to reorganize committee structures will meet, has the added downside of further cleaving off cyber oversight from other oversight activities. If the central concern motivating reform is to consolidate oversight of cyber activities, then this approach makes sense. But what it fails to recognize is that cyber is intertwined with so much else that Congress must oversee. In short, while the Solarium Commission’s proposal integrates the information silos for cyber, it does not solve the more fundamental problem these silos

---

325. See Appendix A: Cyber Operations, *supra* note 173.

326. See *id.*

327. Interview with Congressional Staff Member #4, *supra* note 59.

328. See U.S. CYBERSPACE SOLARIUM COMM’N, *supra* note 20, at 35-36.

create—uninformed legislating for everything else. In fact, it threatens to exacerbate these challenges by creating a new information silo that is even further dissociated from the lawmaking work of the relevant committees.

In short, any effort to take lawmaking authority over cross-jurisdictional matters away from existing committees would meet vigorous opposition.<sup>329</sup> Indeed, similar efforts over the last decade to create select committees on cybersecurity, such as by Senator John McCain in 2011, were unsuccessful;<sup>330</sup> almost every committee leader refused to give up jurisdiction to a select committee.<sup>331</sup> The next Section therefore considers four alternative reforms.

### *B. Four Proposals for Reform*

While a new super committee is not feasible, and perhaps not even desirable, our interviews confirmed that there is increasing awareness among members of Congress and their staff that cross-cutting issues such as drones, special operations, security cooperation, and cyber operations require more inter-committee coordination. In this Section, we propose four reforms that would improve information sharing in Congress. The most significant of these—the creation of a Congressional National Security Council (C-NSC)—would draw on lessons learned from coordinating national security policy within the executive branch.

In proposing reforms, we recognize that any effort at oversight reform will face significant political and administrative hurdles. We acknowledge as well that even if these recommendations were adopted, other oversight challenges would remain. For instance, some critics of congressional oversight over modern warfare activities have pointed out that members of Congress do not have sufficient technical expertise to serve as an effective check on the executive.<sup>332</sup> Underfunded and overstretched staff may lack the

---

329. Interview with Congressional Staff Member #5, *supra* note 22.

330. See Ben Pershing, *On Cybersecurity, Congress Can't Agree on Turf*, WASH. POST (July 18, 2011), [https://www.washingtonpost.com/politics/on-cybersecurity-congress-cant-agree-on-turf/2011/07/18/gIQAQCGWMI\\_story.html](https://www.washingtonpost.com/politics/on-cybersecurity-congress-cant-agree-on-turf/2011/07/18/gIQAQCGWMI_story.html) [<https://perma.cc/NR2U-5VVP>].

331. Interview with Jamil N. Jaffer, *supra* note 27.

332. Molly E. Reynolds, *Improving Congressional Capacity to Address Problems and Oversee the Executive Branch*, BROOKINGS INST. (Dec. 4, 2019), <https://www.brookings.edu/>

bandwidth to engage in rigorous oversight.<sup>333</sup> Prioritizing oversight may be particularly challenging given the lack of political incentives for members of Congress to engage in technical and nuanced national security issues that are not at the forefront of their constituents' concerns. Decreased member interest in intra-party oversight can further limit Congress's efficacy.<sup>334</sup> On the flip side, the executive branch may provide insufficient information to Congress under reporting and notification requirements or may sometimes even refuse to comply with reporting requirements altogether.<sup>335</sup> As an SFRC staffer observed, "You're really at the mercy of the executive branch on what they're willing to share."<sup>336</sup> And yet while these proposed reforms will not solve all the problems that plague congressional oversight of modern warfare, taking steps to address information siloing will tackle an important set of weaknesses in the oversight system. No reform will address all of the

---

policy2020/bigideas/improving-congressional-capacity-to-address-problems-and-oversee-the-executive-branch [<https://perma.cc/A9GR-CDDN>] ("Most individual member offices do not have large enough budgets to consider paying staff members at the maximum level, but the salary cap does affect the ability of committees, especially those with demands for sophisticated expertise, to attract and retain talent.").

333. The challenges posed by the widely acknowledged under-resourcing of congressional staff extend beyond just the national security realm. *See, e.g.*, Alexander C. Furnas & Timothy M. LaPira, *Congressional Brain Drain: Legislative Capacity in the 21st Century*, NEW AMERICA 44 (Sept. 8, 2020), <https://www.newamerica.org/political-reform/reports/congressional-brain-drain/> [<https://perma.cc/LQ7W-EKZQ>] ("The cost of living adjusted wages for entry- and mid-level congressional staff who work 50 hours per week or more is paltry for supposedly the most professional legislature in the world."); Kathy Goldschmidt, *State of the Congress: Staff Perspectives on Institutional Capacity in the House and Senate*, CONG. MGMT. FOUND. 9, 17 (2017), [http://www.congressfoundation.org/storage/documents/CMF\\_Pubs/cmf-state-of-the-congress.pdf](http://www.congressfoundation.org/storage/documents/CMF_Pubs/cmf-state-of-the-congress.pdf) [<https://perma.cc/3LHL-ZUPE>] (noting that "House committees have 50% fewer employees than they did in 1985 and Senate committees have 20% fewer"; only 6 percent of congressional staffers were "very satisfied" with the amount of time and resources allocated to "understand, consider and deliberate policy and legislation").

334. Douglas Kriner, *Can Enhanced Oversight Repair "the Broken Branch"?*, 89 B.U. L. REV. 765, 783 (2009) ("All too often, partisan incentives to support a President of the same party trump institutional incentives to defend Congress's institutional prerogatives by vigorously overseeing the actions of the executive branch.").

335. *See* TODD GARVEY, CONG. RSCH. SERV., R45653, CONGRESSIONAL SUBPOENAS: ENFORCING EXECUTIVE BRANCH COMPLIANCE 1-4 (2019). The trend of executive noncompliance increased significantly during the Trump administration. *See* Fred Kaplan, *Trump's Contempt for Democracy Has Reached New Depths*, SLATE (Jan. 9, 2020, 5:20 PM), <https://slate.com/news-and-politics/2020/01/trump-congress-war-powers-iran.html> [<https://perma.cc/6CH8-STBQ>].

336. Interview with Congressional Staff Member #1, *supra* note 249.

challenges at once, but that is no reason not to aim to make progress where possible. As we stressed at the outset of this Article, information siloing is largely a problem of Congress's own making and thus can be fixed by Congress.<sup>337</sup> That problems may remain in the oversight system is not a justification for failing to take the important steps that are within Congress's power.

### 1. *Expand Cross-Committee Membership*

Congress should expand cross-committee membership. Currently, SSCI includes two members each (one from each party) from SASC, SFRC, judiciary, and appropriations.<sup>338</sup> The armed services, foreign affairs, and intelligence committees should follow the same model, each requiring at least two members (one from each party) from the other two respective committees. For example, SFRC should include at least two members of SASC and two members of SSCI. Similarly, HFAC should include at least two members from HASC and two members from HPSCI. To implement this proposal, Republicans should eliminate their internal rule that senators cannot serve on both SASC and SFRC.<sup>339</sup>

Even more important, the chairs and ranking members of the armed services, foreign relations, and intelligence committees should each serve as *ex-officio*, nonvoting members on the other two respective committees. As one committee staffer explained in an interview, simply having crossover members is insufficient, since one member cannot significantly steer the conversation involving several members who are not read-in to the other committee's affairs.<sup>340</sup> Therefore, committee leadership must also be included. For example, SFRC leadership could serve as *ex-officio*, nonvoting members on both SASC and SSCI. Current rules already allow the chair and ranking member of the SASC to serve as *ex-officio*, nonvoting members on SSCI, so this system simply expands that

---

337. See *supra* Part III.A.

338. *About the Committee*, S. SELECT COMM. ON INTEL., <https://www.intelligence.senate.gov/about#> [<https://perma.cc/UK4U-7B5E>].

339. This proposal focuses on the armed services, intelligence, and foreign relations committees, because, as discussed *supra* notes 33 and 105, they share the vast majority of oversight equities over modern warfare operations.

340. Interview with Congressional Staff Member #1, *supra* note 249.

existing structure.<sup>341</sup> Several congressional staffers interviewed also stressed the need to allow committee staff directors in the room, either in addition to or instead of the members themselves.<sup>342</sup> This recommendation is likely more feasible than large-scale reform, provided that the ex-officio members do not attempt to co-opt oversight.

Moreover, the chair and ranking member of the foreign relations committees should formally be conferees in the NDAA conference process. There is precedent for this practice: two House Democrats from HFAC served on the FY 2020 NDAA conference committee.<sup>343</sup> On the Senate side, however, only members of SASC served on the conference committee.<sup>344</sup> Because nearly all modern warfare regulations today are passed through the NDAA, involvement in the conference process is necessary to shape the oversight regime.<sup>345</sup>

## 2. *Require Joint Briefings*

Although expanding cross-committee membership can facilitate information exchanges, there are times when the full committees should be involved in, or have awareness of, a matter. To this end, Congress should expand and formalize the use of joint briefings and hearings, particularly for cross-cutting, high-stakes issues that implicate the equities of multiple committees.

Joint briefings on overlapping issues can promote holistic and collaborative oversight. A former congressional staff member recalled the benefits of conducting joint briefings following the raid against Osama bin Laden, as members of Congress gained a fuller

341. SENATE RULES, *supra* note 35, R. XXV(4)(b)(3) at 29.

342. Interview with Congressional Staff Member #4, *supra* note 59.

343. Press Release, Nancy Pelosi, Speaker, House of Representatives, Pelosi Names Conferees to National Defense Authorization Act Conference (Sept. 17, 2019), <https://www.speaker.gov/newsroom/91719-1> [<https://perma.cc/6FHS-Y6L7>].

344. *S.1790: National Defense Authorization Act for Fiscal Year 2020*, CONGRESS.GOV, <https://www.congress.gov/bill/116th-congress/senate-bill/1790/all-actions> [<https://perma.cc/V9WY-Q9GM>] (listing “Senate appointed conferees [on Sept. 18, 2019]: Inhofe; Wicker; Fischer; Cotton; Rounds; Ernst; Tillis; Sullivan; Perdue; Cramer; McSally; Scott FL; Blackburn; Hawley; Reed; Shaheen; Gillibrand; Blumenthal; Hirono; Kaine; King; Heinrich; Warren; Peters; Manchin; Duckworth; Jones”).

345. See *supra* Part II.A. All of these proposals would require some additional staff for the committees to manage the extra workload.

picture of the operation: "That was fantastic, because we could trace the intelligence, to targeting, to the operation itself."<sup>346</sup> These "seamless presentations" are not only illuminating for Congress, but they can also force the agencies to coordinate in advance of the briefings and work out any interagency disagreements (as one interviewee pointed out, agencies cannot manipulate their committee patrons to take their position when they brief multiple committees with counterparts from across the government).<sup>347</sup>

There is no reason that joint briefings must be limited to such extraordinary circumstances. The practice of bringing multiple committees together for briefings could become a more regular practice. When multiple agencies are directly involved in an operation, the committees that oversee them and therefore have equities in the matter should be part of the briefing. While the armed services committees may push back on any proposal that dilutes their exclusive access, they may welcome opportunities to gain access to information currently held only by the intelligence committees. In this way, joint briefings could be designed to provide all the relevant committees with access to information that they might otherwise not receive.

### *3. Modify Classification Procedures*

To further facilitate information sharing, Congress should modify rules to allow for sharing of classified information with members and staff when necessary to effective oversight. As Part III explained, when information is classified, it can only be shared on a need-to-know basis as determined by the executive.<sup>348</sup> Classification can prevent members of Congress from sharing certain information with other congressional representatives, and it prevents staff from sharing information across committees.<sup>349</sup> With these rules in place, increasing the number of cross-committee members would have a limited effect. Even though these joint members would know the relevant information, they would still be prohibited from sharing it

---

346. Interview with Congressional Staff Member #6, *supra* note 7.

347. *Id.*

348. *Supra* Part III.A.

349. *See* KAISER, *supra* note 84, at 5-6.

with the rest of the committee.<sup>350</sup> For example, as discussed in Part III, during the Iran crisis concerning the Soleimani strike, Senator Tim Kaine, who is a member of both the SFRC and SASC, knew relevant information about cyber operations from SASC but could not share it with fellow members of the SFRC.<sup>351</sup>

To address this challenge, Congress should reform the rules governing the handling of classified information on the Hill. Specifically, Congress should permit members who have received classified information to share that information with other members and committee staff under clearly defined, limited circumstances.<sup>352</sup> The new rules might mirror the current Executive Order provision that allows for “emergency disclosure” of classified information “when necessary to respond to an imminent threat to life or in defense of the homeland” to “an individual or individuals who are otherwise not eligible for access,” without fully declassifying the information.<sup>353</sup> For example, the law could specify that a “reasonable person would need to find disclosure to the congressional representative or staffer necessary for affecting a lawmaking function.” Though one might be concerned that allowing members to share information would lead to dangerous leaks, setting a clear standard would not only allow Congress to better perform its oversight function but could also provide structure to the already existing informal practice of senators sharing classified information across committees.<sup>354</sup>

350. *See id.*

351. Interview with Congressional Staff Member #1, *supra* note 249.

352. This could be through an amendment to 18 U.S.C. § 798(a) (criminalizing the disclosure of classified information) and/or an addition to the House and Senate rules governing disclosures by HPSCI and SSCI members, respectively. *See* RULES OF THE HOUSE OF REPRESENTATIVES, 114TH CONG., R. X(11)(g), 15 (2015), <https://rules.house.gov/sites/democrats.rules.house.gov/files/114/PDF/House-Rules-114.pdf> [<https://perma.cc/78GJ-7LQ7>]; S. Res. 400, 94th Cong. § 8(a) (1976) (enacted). These rules currently “provide a means for disclosing classified information in the intelligence committees’ possession where the intelligence committee of the respective house (either the House Permanent Select Committee on Intelligence (HPSCI) or the Senate Select Committee on Intelligence (SSCI)) determines by vote that such disclosure would serve the public interest.” JENNIFER K. ELSEA, CONG. RSCH. SERV., RS21900, THE PROTECTION OF CLASSIFIED INFORMATION: THE LEGAL FRAMEWORK 3 (2017).

353. Exec. Order No. 13,526, 75 Fed. Reg. 707, 721-22 (Jan. 5, 2010), *reprinted as amended in* 75 Fed. Reg. 1013 (Jan. 8, 2010).

354. Interview with Congressional Staff Member #5, *supra* note 22.

There is precedent for such a modification. In 2010, a dispute arose when members of the “Gang of Eight” and “Gang of Four” were not permitted to share information with the full intelligence committees.<sup>355</sup> In response, Congress enacted legislation to modify the notification procedures to allow members of the “Gangs” to communicate more fully with members of the intelligence committees.<sup>356</sup> President Obama threatened a veto but ultimately allowed the changes.<sup>357</sup>

In addition to permitting greater information sharing of classified information specifically within Congress, the executive should continue to rein in over-classification.<sup>358</sup> Agency briefers should be required to clarify the classification levels of each part of the briefing. The executive could also institute reforms to disincentivize over-classification, including, for example, clarifying and strengthening classification guidelines; improving classification training for executive branch agencies; reducing penalties for under-classifying; and requiring classifiers to fill out an electronic form that describes the damage classification is seeking to prevent.<sup>359</sup> While the specific details of how to modify classification processes extend beyond the scope of this Article,<sup>360</sup> ensuring that the executive branch clarifies classification levels and only classifies information when absolutely necessary would allow Congress to more easily exchange information, especially when that information does not expose sources and methods. Reforming classification procedures, along with giving

---

355. See KAISER, *supra* note 84, at 6.

356. See Intelligence Authorization Act for Fiscal Year 2010, Pub. L. No. 111-259, § 331(c), 124 Stat. 2654, 2685-86; see also KAISER, *supra* note 84, at 6-7.

357. See Conference Letter regarding S. 1494 and H.R. 2701, the Intelligence Authorization Act for Fiscal Year 2010 from Peter R. Orszag, Dir., Off. of Mgmt. & Budget, to Hon. Dianne Feinstein, Chairwoman, S. Select Comm. on Intel. (Mar. 15, 2010), [https://abcnews.go.com/images/Politics/Letter\\_Orszag\\_to\\_Feinstein\\_100316.pdf](https://abcnews.go.com/images/Politics/Letter_Orszag_to_Feinstein_100316.pdf) [<https://perma.cc/S7BF-VSGR>]; Presidential Statement on Signing the Intelligence Authorization Act for Fiscal Year 2010, 2 PUB. PAPERS 1535 (Oct. 7, 2010).

358. See *Examining the Costs of Overclassification on Transparency and Security: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 69-73 (2016) (statement of Scott Amey, General Counsel, Project on Government Oversight); Doss, *supra* note 266.

359. See Elizabeth Goitein & David M. Shapiro, *Reducing Overclassification Through Accountability*, BRENNAN CTR. FOR JUST. 2-3 (2011), [https://www.brennancenter.org/sites/default/files/2019-08/Report\\_Reducing\\_Overclassification.pdf](https://www.brennancenter.org/sites/default/files/2019-08/Report_Reducing_Overclassification.pdf) [<https://perma.cc/GK9G-TGFX>].

360. For a more detailed discussion of the classification system and recommended modifications to it, see Hathaway, *supra* note 53.

Congress additional flexibility to share information internally, would significantly facilitate the flow of information between related congressional committees.

#### 4. Create a Congressional National Security Council

This brings us to an ambitious, but feasible, proposal: create a *Congressional National Security Council* (C-NSC).

The fundamental challenge that Congress faces is that it has a number of committees with distinct but overlapping jurisdictions. The executive branch faces precisely the same problem: it is made up of a number of agencies with distinct but overlapping jurisdictions. With the National Security Act of 1947, Congress created the National Security Council (NSC) to address this problem for the executive branch while ignoring parallel challenges in Congress. The NSC was designed “to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security.”<sup>361</sup> Initially, NSC members included the President, Secretary of State, the new Secretary of Defense, the Secretary of the Navy, the Secretary of the Air Force, the Chairman of the National Security Resources Board, and other officers “the President may designate from time to time.”<sup>362</sup> Each President has made some changes in NSC membership,<sup>363</sup> but it has always included the key representatives from each agency in the national security space.<sup>364</sup> This allows those agencies to coordinate and cooperate on cross-cutting national security matters. Congress, however, has nothing comparable.

---

361. Pub. L. No. 80-253, § 101(a), 61 Stat. 495, 496 (later codified as amended at 50 U.S.C. § 401 *et seq.*).

362. *Id.* The CIA Director did not initially sit on the NSC, but instead served as an adviser to it. See BEST, *supra* note 21, at 6-7.

363. For example, President Trump’s Director of the CIA sat on the NSC, but in the Biden Administration the Director attends NSC meetings in an advisory capacity. See Eric Geller, *Trump Adding CIA Chief Back to National Security Council*, POLITICO (Jan. 30, 2017, 3:45 PM), <https://www.politico.com/story/2017/01/trump-national-security-council-cia-234381> [<https://perma.cc/3QZX-JCV4>]; Memorandum on Renewing the National Security Council System (NSM-2), 2021 DAILY COMP. PRES. DOC. 1 (Feb. 4, 2021).

364. See generally BEST, *supra* note 21.

There is no reason to accept that asymmetry as inevitable or irreparable. Congress has recognized the need to improve inter-agency coordination within the executive branch on cross-cutting matters.<sup>365</sup> In the FY 2021 NDAA, Congress created the Office of the National Cyber Director (NCD), headed by a Senate-confirmed, cabinet-level official with a seat on the NSC.<sup>366</sup> As the President's principal advisor on cybersecurity, the NCD is charged with coordinating federal government activities on cybersecurity, cyber defense, and related emerging technology issues.<sup>367</sup> Supporters of creating the office envisioned that the NCD would "break down silos across the many agencies with cyber responsibilities."<sup>368</sup> Congress has been willing to compel the executive branch to increase inter-agency coordination—even in the face of presidential opposition.<sup>369</sup> But it has not been as keen about addressing the same issues that it faces internally.<sup>370</sup>

Nothing is stopping Congress from solving the problem of information silos by creating a structure for itself that resembles the NSC. A *Congressional* National Security Council (C-NSC) (or it could be called a "working group"; the name is unimportant) could bring together the leadership of each of the committees involved in national security matters to coordinate on cross-cutting matters, just as the NSC brings together the leadership of the agencies that have equities in planning certain operations or activities.<sup>371</sup> As one interviewee explained, "We do some of this informally. If we see an

---

365. See generally S. REP. NO. 116-236 (2020).

366. FY 2021 NDAA, *supra* note 231, § 1752.

367. See *id.* § 1752(c)(1)(A)-(D).

368. Press Release, Rep. Jim Langevin (D-RI), House of Representatives, National Cyber Director Act Will Be Included in Year-end Defense Bill (Dec. 3, 2020), <https://langevin.house.gov/press-release/national-cyber-director-act-will-be-included-year-end-defense-bill> [<https://perma.cc/8LAM-M6BF>].

369. The Trump administration opposed creating the National Cyber Director, having eliminated the position of the White House cybersecurity coordinator in 2018. See Connor O'Brien & Martin Matishak, *Trump's Defense Veto Would Torpedo Cyber Overhaul Amid Unfolding Hack*, POLITICO (Dec. 18, 2020, 6:00 PM), <https://www.politico.com/news/2020/12/18/trump-veto-ndaa-hack-448492> [<https://perma.cc/A4PU-Z2L8>].

370. Just as its executive branch counterpart, membership of the C-NSC can be flexible. Just as each incoming President has discretion to define what falls within the ambit of national security, briefing on important matters can be tailored to specific committees, or even go beyond the armed services, intelligence, and foreign relations committees where appropriate. See *supra* notes 33, 105.

371. See BEST, *supra* note 21, at 6.

issue come up, we will crosswalk material.”<sup>372</sup> But the interviewee emphasized that this was the exception, not the rule.

The C-NSC would meet periodically to allow its members to brief one another on matters in front of their committees that may be of overlapping interest or in which the actions taken by the agencies under one of their jurisdictions may have implications for decisions before another committee. In the event that the chair and ranking members are stretched too thin, they could deputize a member of the committee to attend in their stead. The key goal would be to create a structure for coordinating and exchanging information across committees rather than relying on happenstance and the decision of one member or staffer to crosswalk information. Of course, it should be clear that sharing information is not an invitation to other committees to extend oversight over matters briefed. Instead, the express purpose should be to better inform committees about matters relevant to their *own* jurisdictions.<sup>373</sup>

The coordination at the member level should be reflected at the staff level as well. Creating a staff-level working group would again mirror the executive branch’s NSC, which coordinates on multiple organizational levels—from working-level staff to principals<sup>374</sup> (although the C-NSC would only have two levels: staff and members). Even if members were not interested in spending the time necessary to establish a member-level C-NSC, such an organization could still be held at the staff level. As one staffer put it, “It should be possible to have staff working groups.”<sup>375</sup> Such a working group would meet on occasion to share information about the matters in front of each committee and coordinate actions as necessary. But the staffer cautioned that a coordinating group would not work unless there is

372. Interview with Congressional Staff Member #5, *supra* note 22.

373. As with any new institutional structure, how well this works will turn in significant part on whether members work within the spirit of the institution—sharing information with one another and respecting committee boundaries. One interviewee made clear that the success of such a proposal will depend on excellent staff setting an appropriate agenda and managing the information flow. Interview with former Congressional Staff Member #6, *supra* note 7. Given the partisanship that mires Congress, establishing the C-NSC would also require buy-in from senior congressional leadership. Members of the C-NSC could also leverage the existing working relationships they have developed in committee as chairs and ranking members of their respective committees to foster information exchanges.

374. See BEST, *supra* note 21, at 1.

375. Interview with Congressional Staff Member #5, *supra* note 22.

awareness and responsiveness to concerns that staff are already stretched thin: "It's a time sink and it's hard and it's an additive function. You would have to increase the budget for committees to hire more staff to do this sort of thing."<sup>376</sup> This is undoubtedly true—any significant reform leading to real improvements in Congress's capacity to properly oversee the executive branch will require additional funding for congressional staff. Likewise, the C-NSC would likely need its own staff, potentially nested under the congressional leadership offices, to set the group's agenda and serve as a secretariat.

Members that are on the C-NSC and their designated staff would need to be given access to all of the relevant classified programs overseen by each of the committees. This alone would significantly facilitate information sharing. If the above proposal to include the chair and ranking member of each of the key committees as ex-officio members on each of the other committees is adopted, then additional classified access would not be required; they would already receive access to allow them to fully participate in C-NSC business. And if they do not, congressional leadership should insist on it.

The advantage of creating this kind of superstructure is that the C-NSC would not take legislative and oversight authority away from the congressional committees. The C-NSC would not be a super committee. In fact, it would not be a committee at all. Rather, like the NSC, the C-NSC would be a coordinating body that exists to allow for regular meetings to consider operations and matters that have cross-jurisdictional effects. The C-NSC would provide a level playing field, where all committee leadership has a seat at the table, no committee has a leading role, and all committees understand the stakes of the matters discussed. This level playing field would significantly facilitate inter-committee dialogue and information exchanges. The proposals recommended above—augment ex-officio membership and permit inter-committee sharing of classified information—would further assist the C-NSC in its work, but their implementation is not essential. What *is* essential is creating space for members to discuss ways in which the matters in front of each

---

376. *Id.*

committee may affect those in front of their own, and learning critical information that they would not otherwise receive through formal reporting channels from the executive branch. As a result, C-NSC members would return to their committees better informed and better prepared to conduct oversight.

Information siloing is ultimately a problem of Congress's own making—the result of political infighting and jurisdictional turf wars. Thus, the onus should be on Congress to ensure that members and committees have the information they need to legislate and properly oversee the executive branch. In comparison to proposals that would require federal agencies to brief more committees, as described in Section IV.A, a C-NSC would make Congress, rather than the executive, responsible for ensuring that information is effectively shared and disseminated. A C-NSC would not even require support from the White House. All it requires is recognition from members of Congress, particularly committee leadership, that coordination and information sharing are essential to overseeing the cross-jurisdictional issues that make up much of modern warfare.

### CONCLUSION

Twenty-first century warfare no longer maps onto committee structures that were created to oversee twentieth-century warfare. Modern military operations do not fit into neat institutional boxes. They are complex and cross-cutting, drawing together intelligence and military tools, techniques, and assets to respond to threats abroad.

As this Article has shown, jurisdictional turf battles and rigid classification rules inhibit adequate information sharing across Congress. Jurisdictional jealousies and the realities of legislating today through the NDAA process have produced information silos that impede Congress's ability to effectively perform its oversight responsibilities. Modern warfare in particular has brought this pathology to the fore. As a result, today's oversight system is one in which many congressional committees know something about significant military and covert action operations, but no member of Congress is in a position to put all these pieces together.

This is not merely a concern for constitutional formalists, who worry about the effect this has on Congress's capacity to exercise its constitutional obligations. It also has real-world effects, leading to situations like the tragedy in Niger described at the outset of this Article<sup>377</sup> or Senator Tim Kaine's inability to share vital information related to the killing of Major General Soleimani from a classified SASC briefing with his colleagues on the SFRC.<sup>378</sup> In short, Congress's inability to gain a complete picture of modern warfare operations and capabilities harms the U.S. government's ability to protect U.S. national security.

But if the bad news is that this problem is of Congress's own making, the good news is that it is within the power of Congress to fix it. If Congress wishes to conduct effective oversight over a rapidly evolving set of modern warfare capabilities, it must bring down the walls that stand in the way of adequate information sharing. In 1947, Congress recognized the importance of cooperation among executive branch agencies working on national security matters, and it passed legislation that gave rise to a new National Security Council to encourage information sharing, collaboration, and cooperation across executive branch agency boundaries. It is time for Congress to bring the same revolution to its own institutional structures.

---

377. *See supra* notes 1-7 and accompanying text.

378. *See supra* notes 259-60 and accompanying text.