CYBERSECURITY INFORMATION SHARING AND CONGRESS'S OVERSIGHT ROLE

JONATHAN LEWALLEN†

ABSTRACT

"Information sharing" has arisen as a common policy alternative within issues related to homeland security and terrorism, including cybersecurity. Congress has used laws and executive reorganization to encourage federal agencies to more effectively share information about cyber vulnerabilities and threats with each other, with state and local governments, and with private sector businesses, and to encourage

† Assistant Professor, University of Tampa. The author thanks Meagan Dreher and *Wayne Law Review* for their editorial support.

businesses to share more information with the government. By enhancing direct communication between agencies and businesses, Congress can encourage flexible, adaptive responses without needing to frequently revise existing law to incorporate new threats and vulnerabilities. However, doing so limits the institution's role in overseeing cybersecurity policy. Information sharing as a policy alternative does not fit neatly within frameworks for understanding congressional oversight, and many of the oversight tools at Congress's disposal either do not apply or are less effective when applied to cybersecurity information sharing. This Article analyzes those frameworks, tools, and challenges as well as why legislators would support an option that limits their role and puts them at an information disadvantage; it also examines the implications for both the practice and study of congressional oversight.

I. INTRODUCTION

Congress enacted the Cybersecurity Act of 2015 as part of the omnibus 2016 Consolidated Appropriations Act.[1] Title I of the Cybersecurity Act required the leaders of multiple federal agencies to develop procedures for sharing information about cybersecurity threats, vulnerabilities, and best practices with other agencies and with non-federal actors, including state, local, tribal, and territorial governments as well as private entities.[2] The law also includes language that allows private entities to both share information about cyber threats and defensive measures with other private entities and the federal government and to operate certain defensive measures against cyber threats.[3]

The focus on information sharing as a policy alternative[4] has grown in popularity following the September 11, 2001, terrorist attacks. In their

1. Cybersecurity Act of 2015, Pub. L. No. 114-113, Div. N, tit. I, 129 Stat. 2935 (current version at 6 U.S.C. §§ 1501–1510 (2018)).

2. *Id.* The law puts the Director of National Intelligence, Secretaries of Defense and Homeland Security, and the Attorney General in charge of developing the procedures in consultation with the Secretaries of Commerce, Energy, and the Treasury.

3. *Id.*

4. I follow the definition of "policy alternative" as a choice or course of government action referred to in JOHN W. KINGDON, AGENDAS, ALTERNATIVES, AND PUBLIC POLICIES 4, 4 n.2 (1984). Other scholars may use "solution" to describe a policy proposal; however, doing so implies that the problem can be solved rather than mitigated or managed, which may not be appropriate for cybersecurity. *See* Kiersten E. Todt, *What We Continue to Get Wrong About Cybersecurity*, FIFTHDOMAIN.COM (Oct. 14, 2019), https://www.fifthdomain.com/opinion/2019/10/14/what-we-continue-to-get-wrong-about-cybersecurity/

report on the circumstances surrounding the attacks, the 9/11 Commission made a series of recommendations for U.S. global strategy and government organization.[5] One of the latter was "unity of effort in sharing information," in which the commission recommended that information be shared "horizontally" across agencies to a greater degree.[6] Over the past two decades, the U.S. government has adopted multiple information sharing policies for terrorism and homeland security-related issues. The Homeland Security Act of 2002 established mechanisms for sharing information related to homeland security, critical infrastructure, and foreign intelligence.[7] A 2003 presidential executive order required agencies to develop common standards for sharing terrorism-related information with state, local, tribal, and territorial (SLTT) governments.[8] The Intelligence Reform and Terrorism Prevention Act from the same year also created an "Information Sharing Environment," which includes agencies ranging from the Department of Homeland Security and the Federal Bureau of Investigation, to the Departments of Interior and Health and Human Services.[9] The Government Accountability Office (GAO) added information sharing to their "High-Risk List" in 2005 to highlight the lack of clear plans and consistent objectives across agencies.[10] In 2012, President Barack Obama issued his *National Strategy for Information Sharing and Safeguarding*, in which he declared information a "national asset."[11] The Chemical Facility Anti-Terrorism

---

[http://web.archive.org/web/20200321205323/https://www.fifthdomain.com/opinion/2019/10/14/what-we-continue-to-get-wrong-about-cybersecurity/].

5. THE NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004) [hereinafter *9/11 Report*], https://www.9-11commission.gov/report/911Report.pdf [http://web.archive.org/web/20200421191938/https://www.9-11commission.gov/report/911Report.pdf].

6. *Id.* "Information sharing" as a policy alternative existed prior to the 9/11 Commission report, such as when the Anti-Drug Abuse Act of 1988 created "High Intensity Drug Tracking Areas" to help coordinate federal anti-drug trafficking efforts with state and local governments. *See* Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, tit. VI, § 6101(a), 102 Stat. 4181 (1988) (codified as amended at 34 U.S.C. § 10321 (2017).

7. Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135 (codified at 6 U.S.C. § 101 (2012)).

8. Exec. Order No. 13311, 68 Fed. Reg. 45,149 (July 29, 2003).

9. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (codified at 50 U.S.C. § 401 (2011)).

10. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-207, HIGH RISK SERIES: AN UPDATE (2005).

11. President Barack Obama, *National Strategy for Information Sharing and Safeguarding* 6 (2012), https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy_1.pdf

Standards (CFATS) Act of 2014 established an executive branch working group charged with improving chemical facility operators' access to information and data about potential terrorist threats, among other items.[12]

Although Congress has encouraged the adoption of information sharing, including the Cybersecurity Act of 2015, it challenges our understanding of how Congress oversees laws, regulations, and the private sector. Representative Elissa Slotkin (D-Mich.) put it directly in a 2019 hearing on CFATS:

> [H]ow would a Member of Congress know . . . if the facilities in his or her district have communicated effectively with local law enforcement? . . . I get a lot of, I guess they'd call them complaints, from the people back home generally about the lack of information sharing between folks in Washington seeing some of the top-secret or secret-level information on threats related to cyber and then what actually distills down.[13]

Moreover, the nature of cybersecurity as a policy problem and the current approaches to its regulation present challenges for effective congressional oversight of cybersecurity information sharing. Many of the tools Congress traditionally uses to foster compliance also would diminish the policy's effectiveness in this case. Because the U.S. government relies on technology and software provided by the private sector, the government itself can be left vulnerable when companies do not share information about vulnerabilities and threats,[14] yet the overall U.S. stance has been to limit its regulation of technology development and the Internet.[15]

[http://web.archive.org/web/20200421192423/https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy_1.pdf].

12. The Chemical Facility Anti-Terrorism Standards Act of 2014, Pub. L. No. 113-254, 128 Stat. 2898 (codified at 6 U.S.C. §§ 621–629 (2019)).

13. *Securing Our Nation's Chemical Facilities: Building on the Progress of CFATS Program: Hearing Before the H. Comm. on Homeland Security*, 116th Cong. (2019) [hereinafter *Securing Our Nation's Chemical Facilities*] (question from Rep. Elissa Slotkin, D-Mich).

14. Sean Lyngaas, *Senators Question Vulnerability Disclosure Process After Spectre and Meltdown Stumbles*, CYBERSCOOP (July 11, 2018), https://www.cyberscoop.com/senators-question-vulnerability-disclosure-process-spectre-meltdown-stumbles/
[http://web.archive.org/web/20200321225618/https://www.cyberscoop.com/senators-question-vulnerability-disclosure-process-spectre-meltdown-stumbles/].

15. *See* Shaun Waterman, *Who's in Charge of Regulating the Internet of Things?*, CYBERSCOOP (Oct. 26, 2016), https://www.cyberscoop.com/iot-security-regulators-mirai-

This Article proceeds in four parts. In order to illustrate how and why cybersecurity information sharing as a policy alternative poses challenges for congressional oversight, I must define and describe how oversight works. The second part delineates competing conceptions of congressional oversight and the different oversight tools at Congress's disposal.[16] Such tools include hearings, veto over nominations, and administrative "deck stacking."[17] I next describe how information sharing has developed and expanded as a policy alternative within the cybersecurity domain as well as the current obstacles for participation and compliance in information sharing among federal agencies, state and local governments, and private businesses.[18] The fourth part details the different challenges cybersecurity information sharing poses to congressional oversight.[19] Some of the challenges are general, such as how success might be measured and the changing nature of what information might be shared, while others are specific to individual oversight tools.[20] Much of congressional oversight relies on the possibility of future legislation for its effectiveness; the nature of information sharing as an approach to policy blunts some of that threat and, as Representative Slotkin noted, reinforces Congress's information disadvantage.[21] The final part comments on the implications of "information sharing" as a policy alternative for both the practice and the study of congressional oversight.[22]

II. CONGRESSIONAL OVERSIGHT: DEFINITIONS AND TOOLS

Congressional oversight is based in the institution's Constitutional legislative powers and on Congress's need to deal with a complex policy environment in a way that allows members to claim credit for solving problems.[23] Arguing against annual House elections in *Federalist 53*,

---

botnet/ [https://web.archive.org/web/20200331054157/https://www.cyberscoop.com/iot-security-regulators-mirai-botnet/] (discussing how high publicity cyber-attacks have put pressure on the U.S. government to take action).

16. *See infra* Part II.
17. *See infra* Part II.B.
18. *See infra* Part III.
19. *See infra* Part IV.
20. *See infra* Part IV.
21. *See Securing Our Nation's Chemical Facilities*, *supra* note 13.
22. *See infra* Part V.
23. Watkins v. United States, 354 U.S. 178 (1957); McGrain v. Daugherty, 273 U.S. 135 (1927); MORRIS P. FIORINA, CONGRESS: KEYSTONE OF THE WASHINGTON ESTABLISHMENT (Yale Univ. Press 1977); Mathew D. McCubbins & Talbot Page, *The Congressional Foundations of Agency Performance*, 51 PUB. CHOICE 173, 173–90

James Madison, writing as Publius, noted that "[n]o man can be a competent legislator who does not add to an upright intention and a sound judgment a certain degree of knowledge of the subject on which he is to legislate."[24] But whereas Madison also believed that "[t[he most laborious task will be the proper inauguration of the government and the primeval formation of a federal code. Improvements on the first draught will every year become both easier and fewer,"[25] Congress's policy environment has become more complex. That complexity often requires more sustained attention and greater expertise than members of Congress can provide within a two- or six-year term. Moreover, the Constitution delegates the responsibility to "take Care that the Laws be faithfully executed" to the executive in Article II.[26] Congress thus delegates responsibility for implementing laws, and often responsibility for developing policy specifics, to federal, state, and local agencies. Such delegation may involve specifying the scope and instruments of agency authority or the procedures agencies must follow in working towards the legislature's policy goals.[27] Delegation then requires oversight to ensure that Congress's goals are being met.[28] Despite oversight being a core congressional function, a standard definition has proved elusive.[29] This part will begin with a brief discussion regarding the competing conceptions of congressional oversight and then describe specific oversight tools at Congress's disposal.[30]

A. Competing Definitions of Oversight

Congressional oversight has been defined differently by various scholars. In its broadest conception, we might think of oversight as

---

(1986); David H. Rosenbloom, *"Whose Bureaucracy Is This, Anyway?" Congress' 1946 Answer*, 34 POL. SCI. & POLS. 773, 773–77 (2001).

24. THE FEDERALIST NO. 53, at 397 (James Madison) (1987).

25. *Id.* at 329.

26. U.S. Const. art. II, § 3, cl. 5.

27. McCubbins & Page, *supra* note 23, at 176–77.

28. *See Congressional Oversight: An Overview*, EVERYCRSREPORT.COM (Feb. 10, 2010), https://www.everycrsreport.com/reports/R41079.html [https://web.archive.org/web/20200612060222/https://www.everycrsreport.com/reports/R41079.html].

29. *See* Mark Strand & Tim Lang, *Executive Oversight: Congress' Oft-Neglected Job*, CONG. INST. (Nov. 11, 2011), https://www.congressionalinstitute.org/2011/11/28/executive-oversight-congress-oft-neglected-job/ [https://web.archive.org/save/https://www.congressionalinstitute.org/2011/11/28/executive-oversight-congress-oft-neglected-job/].

30. *See infra* Parts II.A–B.

"behavior by legislators and their staffs, individually or collectively, which results in an impact, *intended or not*, on bureaucratic behavior."[31] This definition allows us to focus on bureaucratic behavior rather than on Congress's intent, the latter of which may be hard to determine simply by observing the former; indeed, members of Congress may not have a particular outcome in mind and prefer to control the process by which bureaucratic decisions are made.[32] Such activities also would include the nominations process, in which the Senate plays a role in selecting the agents who will direct policy implementation, and administrative "deck stacking"—enfranchising certain groups within the regulatory process to ensure that administrators respond to those interests.[33] Oversight activity might similarly include legislation, if one thinks of the former as "activity that forces some patterned response by executive branch officials."[34] If we were to adopt the broad definition of oversight, however, all congressional activities could potentially be considered oversight, thus rendering the definition unhelpful.[35]

More limited definitions conceive of congressional oversight as review of policy implementation and agency decisions after they have been made.[36] Many studies of delegation and oversight rely on a principal-agent model from the study of organizations, in which Congress must engage in monitoring to ensure agency compliance.[37] Even within that context, however, scholars have disagreed over whether such monitoring must be constant for Congress to adequately meet its Constitutional responsibilities. Rather than engage in active, regular "police patrols" of administrative activities, Congress can rely on constituents, organized interests, and other groups to participate in the implementation process and sound "fire alarms" to notify Congress of

---

31. MORRIS S. OGUL, CONGRESS OVERSEES THE BUREAUCRACY: STUDIES IN LEGISLATIVE SUPERVISION 11 (Univ. of Pittsburgh Press 1976) (emphasis added).

32. CHRISTOPHER H. FOREMAN, Jr., SIGNALS FROM THE HILL: CONGRESSIONAL OVERSIGHT AND THE CHALLENGE OF SOCIAL REGULATION (Yale Univ. Press 1989); Mathew D. McCubbins et al., *Administrative Procedures as Instruments of Political Control*, 3 J.L. ECON. & ORG. 243, 244, 255 (1987).

33. Randall L. Calvert et al., *A Theory of Political Control and Agency Discretion*, 33 AM. J. POL. SCI. 588, 588–611 (1989).

34. Leon Halpert, *Legislative Oversight and the Partisan Composition of Government*, 11 PRESIDENTIAL STUD. Q. 479 (1981).

35. OGUI, *supra* note 31, at 11.

36. JOEL D. ABERBACH, KEEPING A WATCHFUL EYE: THE POLITICS OF CONGRESSIONAL OVERSIGHT (Brookings Inst. Press 1990); FOREMAN, *supra* note 32. However, Foreman also argues that legislation vs. oversight represents a false dichotomy.

37. Terry M. Moe, *The New Economics of Organization*, 28 AM. J. POL. SCI. 739, 739–77 (1984).

where it should devote its oversight attention.[38] Monitoring or supervision itself may not suffice, as McCubbins and Schwartz characterize oversight as Congress's "attempts to detect *and remedy* executive-branch violations of legislative goals."[39]

Delegation to expert bureaucracies creates an information asymmetry; agencies know more about the subjects under their authority and could potentially use that knowledge to evade effective oversight.[40] "Fire alarms" help mitigate the asymmetry, but Congress also can require periodic reports and appeal to bureaucrats' professional norms as means of revealing the latter's information. While the principal-agent model of delegation and oversight emphasizes the importance of rewards and sanctions to incentivize bureaucratic behavior, oversight does not have to be adversarial; bureaucracies help reduce legislator uncertainty about the nature of a policy problem, and a committee and agency may have common policy aims.[41]

While congressional oversight typically refers to interactions with the executive branch, Levin and Bean included in their definition of oversight "the full range of inquiries conducted by Congress, whether short or long term, routine or special, targeting the public *or private* sector."[42] Their definition is broader, not in the range of congressional activities that may qualify as oversight, but in the range of activities overseen.[43] Therefore, Levin and Bean called attention to areas of self- and co-regulation where Congress may not have delegated authority to

---

38. Mathew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 165–79 (1984); Barry R. Weingast, *The Congressional-Bureaucratic System: A Principal Agent Perspective (with Applications to the SEC)*, 44 PUB. CHOICE, 147, 147–91 (1984). However empirical evidence suggests police patrol-style oversight does occur. *See generally* Steven J. Balla & Christopher J. Deering, *Police Patrols and Fire Alarms: An Empirical Examination of the Legislative Preference for Oversight*, 40 CONG. & PRESIDENCY 27 (2013) (discussing the results of their empirical study of congressional oversight, which indicate a substantial amount of "police patrol" oversight).

39. McCubbins & Schwartz, *supra* note 38, at 165 (emphasis added).

40. *See* John D. Huber & Charles R. Shipan, *Politics, Delegation, and Bureaucracy*, *in* OXFORD HANDBOOK POL. ECON. 256 (Barry R. Weingast & Donald Wittman eds., Oxford 2006).

41. SAMUEL WORKMAN, THE DYNAMICS OF BUREAUCRACY IN THE US GOVERNMENT: HOW CONGRESS AND FEDERAL AGENCIES PROCESS INFORMATION AND SOLVE PROBLEMS (Cambridge Univ. Press 2015); John P. Bradley, *Shaping Administrative Policy with the Aid of Congressional Oversight: The Senate Finance Committee and Medicare*, 33 W. POL. Q. 492, 500–01 (1980); Samuel Workman et al., *Problem Definition and Information Provision by Federal Bureaucrats*, 43 COGNITIVE SYS. RES. 140 (2017).

42. Former Senator Carl Levin & Elise Bean, *Defining Congressional Oversight and Measuring Its Effectiveness*, 64 WAYNE L. REV. 1, 1 n.2 (2018) (emphasis added).

43. *Id.*

an agency, but it nevertheless has some policy goal it wishes pursued.[44] Given the nature of information sharing as a policy alternative, this Article defines congressional oversight as those actions intended to either monitor or affect the activity of those at whom the oversight is directed, whether the federal bureaucracy, state and local governments, or the private sector. This Article only considers public (observable) actions and sets aside informal staff interactions and similar latent activities. Further, this Article does not include oversight by legislative support agencies such as the Government Accountability Office or Inspectors General, though they undoubtedly are key contributors to Congress's oversight capacity.

B. Congress's Oversight Tools

Given this Article's working definition of oversight, Congress has several tools at its disposal to try to achieve its goals, including committee hearings; investigations and other reports; Senate approval or veto of executive and judicial nominations; administrative "deck stacking"; casework; and the authorization-appropriations process.[45] While this list is not meant to be exhaustive, it provides a representative range of oversight-related activities.

1. Hearings

Committee hearings can serve multiple purposes for congressional oversight. Hearings allow members to learn about the issues under their jurisdiction and establish a record of facts that can then help reduce the information asymmetry with the bureaucracy.[46] Some of that information comes from bureaucracies themselves, particularly when committees are uncertain about how to define a policy problem.[47] Hearings also act as an indicator of priorities and can shift an agency's attention to a committee's preferred issue.[48] Hearings further serve an oversight

44. *See id.* at 10–11 (discussing congressional oversight of both public and private sector activities).

45. *See infra* Parts I.B.1–4.

46. ELISE J. BEAN, FINANCIAL EXPOSURE: CARL LEVIN'S SENATE INVESTIGATIONS INTO FINANCE AND TAX ABUSE (Palgrave Macmillan 2018); ROBERT G. KAISER, ACT OF CONGRESS: HOW AMERICA'S ESSENTIAL INSTITUTION WORKS, AND HOW IT DOESN'T (Vintage 2013).

47. WORKMAN, *supra* note 41; Workman et al., *supra* note 41.

48. Peter J. May et al., *Organizing Attention: Responses of the Bureaucracy to Agenda Disruption*, 18 J. PUB. ADMIN. RES. & THEORY: J-PART 517, 520-21 (2008); Jeff Worsham & Jay Gatrell, *Multiple Principals, Multiple Signals: A Signaling Approach to Principal-Agent Relations*, 33 POL'Y STUD. J. 363, 363–76 (2005).

purpose through the witnesses that testify and answer member questions.[49] Committee members can directly confront bureaucrats and private sector actors and call on "careerists," interest groups, citizens, and other legislators to provide multiple types of information and counteract "uninformative" political appointees.[50] By bringing in a variety of witnesses, committees broaden participation in the political process and enhance congressional representation of issue, district, and state interests.[51] Oversight hearings also can deter future actions; recordings of a series of hearings investigating money laundering at Citigroup in the 1990s were later used internally by the company as a warning against finding itself in that position again.[52] Committees tend to find oversight hearings worthwhile both during periods of ideological conflict between the committee and agency as well as when working with a like-minded agency to undo the previous administration's regulations.[53]

2. Investigations

As with hearings, committees and subcommittees typically conduct congressional investigations. Investigations may result in hearings or written reports (or both), and investigations typically require a significant investment of committee time, staff, and other resources.[54] Committee or subcommittee chairs and their staff typically lead investigations, though the ranking member (top-ranking minority party member on the committee) also often provides support and occasionally suggests topics.[55] Investigations could cover routine public sector and private sector matters or respond to singular events like scandals or disasters.[56]

---

49. *See* Paul Burstein & C. Elizabeth Hirsh, *Interest Organizations, Information, and Policy Innovation in the U.S. Congress*, 22 SOC. F. 174, 179 (2007); Jonathan Lewallen, *Congressional Attention and Opportunity Structures: The Select Energy Independence and Global Warming Committee*, 35 REV. OF POL'Y RES. 153, 153–69 (2018); Foreman, *supra* note 32.

50. *Id.*

51. *See* Burstein & Hirsch, *supra* note 49, at 185–86 (reporting the diversity of witnesses before congressional committees).

52. BEAN, *supra* note 46.

53. Jason A. MacDonald & Robert J. McGrath, *Retrospective Congressional Oversight and the Dynamics of Legislative Influence Over the Bureaucracy*, 41 LEG. STUD. Q. 899, 900–01 (2016); Robert J. McGrath, *Congressional Oversight Hearings and Policy Control*, 38(3) LEGIS. STUD. Q. 349, 353–54 (2013).

54. BEAN, *supra* note 46.

55. David C.W. Parker & Matthew Dull, *Rooting Out Waste, Fraud, and Abuse: The Politics of House Committee Investigations, 1947-2004*, 66 POL. RES. Q. 630, 630–44 (2013); *see also id.*

56. Levin & Bean, *supra* note 42.

Committee investigations into executive branch activities can act as a check on presidential power, while investigations into government contractors and private sector actors can generate publicity and credit—key motivations for congressional behavior.[57] Perhaps because of the time required to conduct effective investigations, they have become more common in the Senate than in the House of Representatives since the mid-1990s. However, the rise of judicial review of agency decisions (facilitated by Congress) alleviates some of the need for congressional review of same.[58] Individual legislators have discretion over how to allocate their office resources, and some might prioritize investigations and similar reports; former Senator Tom Coburn (R-OK), for example, issued annual "Wastebooks" and other reports into government spending (though note a distinction between these individual investigations and casework, described below).[59]

3. Nominations/Appointments

The U.S. Constitution's "advice and consent" clause essentially gives the Senate a veto over executive and judicial branch nominations, and this power is an important tool for congressional oversight.[60] In a principal-agent framework, "selecting the right agent" is often a more efficient way for the principal to obtain her preferred outcome; if the agent and principal agree on desirable outcomes, the latter does not need to spend time monitoring the former.[61] Some scholars in this tradition find that—even in formal theoretic models of legislative and executive bargaining over agency policy that include a post-decision veto over the selected policy, unilateral executive power to "fire" a recalcitrant agent, or other means of political control—the initial appointment stage is most important for determining the policy outcomes reached.[62] Even if they do

---

57. DOUGLAS KRINER & ERIC SCHICKLER, INVESTIGATING THE PRESIDENT: CONGRESSIONAL CHECKS ON PRESIDENTIAL POWER (Princeton Univ. Press 2017); John I. Hanley, Legislative Limelight: Investigations by the United States Congress (2012) (Ph.D. dissertation, University of California, Berkeley).

58. Hanley, *supra* note 57; *see also* THE FEDERALIST NO. 63 (Alexander Hamilton) (writing about the need for a body in the legislature "having sufficient permanency to provide for such objects as require a continued attention").

59. Emma Dumain, *Coburn Pushes for Funding Boost to GAO*, ROLLCALL.COM (Nov. 15, 2011, 6:25 PM), https:/www.rollcall.com/2011/11/15/coburn-pushes-for-funding-boost-to-gao/ [https://web.archive.org/web/20200307211336/https:/www.rollcall.com/2011/11/15/coburn-pushes-for-funding-boost-to-gao/].

60. U.S. CONST. art. II, § 2, cl. 2.

61. Calvert et al., *supra* note 33.

62. *Id.*; Weingast, *supra* note 38.

not reject a nominee, senators can strategically delay a nomination in order to "protect" an agency from shifting its policies towards the president's preferred outcomes.[63]

4. "Deck-Stacking"

Congress can use administrative procedures to both reduce its information disadvantage relative to the bureaucracy and prevent future coalitions from shifting policy; that is, it "stacks the deck" against deviation from whatever policy bargain was struck.[64] Congress can stack the deck in several ways: requiring a "notice and comment" period during preliminary rulemaking that notifies Congress of what actions are being considered and allows different interests to communicate their views; imposing strict evidentiary standards on rulemaking that limit agency discretion, including legislative provisions for judicial review of agency decisions, which provides parties with aligned interests an additional venue in which to make their voices heard; and creating federal advisory committees with guaranteed membership for representatives of certain interests.[65] In stacking the deck in favor of groups central to the policy enacting coalition, however, administrative procedures provide points of access for future legislators to reverse the enacting coalition's preferred policy and to increase the enacting coalition's transaction costs, along with everyone else's.[66]

5. Casework

Constituency service, or casework, is an important tool of congressional oversight available to individual legislators even if they lack committee and subcommittee resources.[67] Legislators typically have staff both in D.C. and in their districts or states devoted to responding to

63. Ian Ostrander, *The Logic of Collective Inaction: Senatorial Delay in Executive Nominations*, 60 AM. J. POL. SCI. 1063, 1063–76 (2016).

64. JERRY L. MASHAW, GREED, CHAOS, AND GOVERNANCE: USING PUBLIC CHOICE TO IMPROVE PUBLIC LAW 120–21 (Yale Univ. Press 1997).

65. Steven J. Balla & John R. Wright, *Interest Groups, Advisory Committees, and Congressional Control of the Bureaucracy*, 45 AM. J. POL. SCI. 799, 799–812 (2001); McCubbins et al., *supra* note 32.

66. Murray J. Horn & Kenneth A. Shepsle, *Commentary on "Administrative Arrangements and the Political Control of Agencies": Administrative Process and Organizational Form as Legislative Responses to Agency Costs*, 75 VA. L. REV. 499, 499–508 (1989).

67. SARAH J. ECKMAN, CONG. RESEARCH SERV., R44726, CONSTITUENT SERVICES: OVERVIEW AND RESOURCES (2017), https://fas.org/sgp/crs/misc/R44726.pdf [http://web.archive.org/web/20200424215332/https://fas.org/sgp/crs/misc/R44726.pdf].

constituent requests for intercession with the executive branch.[68] In 1946, casework took up between fifty and seventy-five percent of a member's time, and staff dedicated to casework, particularly in district and state offices, increased in the ensuing decades.[69] Intercessions might range from ensuring a constituent receives an overdue Social Security check to advocating that a government contract be awarded to a small business in a legislator's district; depending on the constituent communication involved, casework can represent a legislator's response to a "fire alarm" as described above.[70] Casework can lead to additional oversight or legislative action, with House members more likely than senators to find casework "very effective" for that purpose.[71] Casework can also highlight problems in field offices for higher-ranking agency administrators.[72]

6. Authorization and Appropriations

Congress's "power of the purse" acts in part as a system of rewards or sanctions for agency compliance with legislative goals and directives.[73] Congressional spending is split into two related, but separate, processes: authorization, in which Congress determines how much money an agency is allowed to spend in a given fiscal year; and appropriations, in which Congress actually provides the specific dollar

68. Alan Rosenthal, *Beyond the Intuition That Says "I Know One When I See One," How Do You Go About Measuring the Effectiveness of Any Given Legislature?*, NCSL.ORG (1999), https://www.ncsl.org/research/about-state-legislatures/the-good-legislature.aspx [https://web.archive.org/web/20200613174715/https://www.ncsl.org/research/about-state-legislatures/the-good-legislature.aspx].

69. Molly E. Reynolds, *Vital Statistics on Congress: Data on the U.S. Congress, Update March 2019*, BROOKINGS.EDU (Mar. 4, 2019), https://www.brookings.edu/multi-chapter-report/vital-statistics-on-congress/ [http://web.archive.org/web/20200421195049/https://www.brookings.edu/multi-chapter-report/vital-statistics-on-congress/].

70. *Office of Small and Disadvantaged Business Utilization*, SOC. SEC. ADMIN., https://www.ssa.gov/osdbu/faqs.html [http://web.archive.org/web/20200421195127/https://www.ssa.gov/osdbu/faqs.html] (last visited Mar. 22, 2020).

71. R. ERIC PETERSEN & SARAH J. ECKMAN, CONG. RESEARCH SERV., RL33209, CASEWORK IN A CONGRESSIONAL OFFICE: BACKGROUND, RULES, LAWS, AND RESOURCES (2017), https://fas.org/sgp/crs/misc/RL33209.pdf [https://web.archive.org/web/20180606004646/https://fas.org/sgp/crs/misc/RL33209.pdf].

72. John R. Johannes, *Casework as a Technique of U.S. Congressional Oversight of the Executive*, 4 LEG. STUD. Q. 325, 325–51 (1979).

73. McCubbins & Page, *supra* note 23; Weingast, *supra* note 38.

amounts agencies have to spend.[74] Importantly, these two processes are governed by different sets of committees: the Appropriations Committees in each chamber handle the latter, while the different committees with jurisdiction over the agency or agencies in question handle the authorization process.[75] The budget process provides an observable, quantifiable measure of agency resources; if Congress determines that policy outcomes are not in line with those resources, it can adjust an agency's budget accordingly. Beyond any effect of specific changes to budgetary resources, the authorization and appropriations processes provide opportunities for regular monitoring of agency behavior. Given limits on legislator time and attention, setting programs to expire after a certain number of years, unless they are reauthorized, allows Congress to review the authority it has delegated to the executive branch and claim credit for having addressed pressing policy problems.[76] The appropriations process provides similar opportunities, though again, it does not have to be adversarial; indeed, repeated interactions between committees and agencies over time lead to anticipated reactions and shared budgetary expectations.[77]

Having described different congressional oversight tools, this Article now turns to U.S. cybersecurity policy and reliance on information sharing as a policy alternative.[78] It then discusses how cybersecurity information sharing poses challenges for effective congressional oversight across its range of tools.[79]

---

74. *Legislative Process 101—Authorization vs. Appropriation*, INDIVISIBLE, https://indivisible.org/resource/legislative-process-101%E2%80%94authorization-vs-appropriation [http://web.archive.org/web/20200421195359/https://indivisible.org/resource/legislative-process-101%E2%80%94authorization-vs-appropriation].

75. Each chamber also has a Budget Committee responsible for drafting an annual budget resolution, but this resolution is nonbinding and thus merely represents a statement of congressional policy priorities. *See The Federal Budget: Understanding the Terms and the Players*, NAEYC.ORG, https://www.naeyc.org/our-work/public-policy-advocacy/the-federal-budget-understanding-the-terms-and-the-players [https://web.archive.org/web/20200606170001/https://www.naeyc.org/our-work/public-policy-advocacy/the-federal-budget-understanding-the-terms-and-the-players].

76. E. SCOTT ADLER & JOHN D. WILKERSON, CONGRESS AND THE POLITICS OF PROBLEM SOLVING (2012); JAMES H. COX, REVIEWING DELEGATION: AN ANALYSIS OF THE CONGRESSIONAL REAUTHORIZATION PROCESS (2004); THAD HALL, AUTHORIZING POLICY (2004).

77. AARON WILDAVSKY, THE NEW POLITICS OF THE BUDGETARY PROCESS (2d ed. 1992); Otto A. Davis et al., *A Theory of the Budgetary Process*, 60 THE AM. POL. SCI. REV. 529, 529–47 (1966); Bryan D. Jones et al., *Does Incrementalism Stem from Political Consensus or from Institutional Gridlock?*, 41 AM. J. POL. SCI. 1319, 1319–39 (1997).

78. *See infra* Part III.

79. *See infra* Part IV.

III. CYBERSECURITY AND INFORMATION SHARING

In order for policymakers to act—whether through legislation, regulation, or some other means—they first must agree on how the problem is defined. Yet cybersecurity lacks a consistent, agreed-upon definition.[80] As a policy problem, cybersecurity's issue dimensions are driven by changes in technology. Cybersecurity involves concerns about securing both digital data and the networks and "clouds" through which such data can be accessed, manipulated, and transferred. The core concern that unites cybersecurity's disparate components is *vulnerability*: of data, of networks, and of operations or systems.[81] As technology emerges and changes, older systems may be vulnerable to unauthorized access, vandalism, theft, manipulation, and exploitation by new threats, while newer systems and software may be vulnerable due to inadequate testing or intentional vulnerabilities introduced along the supply chain.[82] Protection against different potential vulnerabilities is the "security" in cybersecurity. Data and network security each have domestic and foreign policy concerns depending on the source of the threat. The lack of agreement on how to define cybersecurity extends internationally, as the U.S. and other Western countries think of cybersecurity as a technical problem while countries such as China, Russia, and Saudi Arabia include a broader concern for control over information, though the U.S. military

---

80. Jule Lowrie, *Cybersecurity: A Primer of U.S. and International Legal Aspects*, *in* CYBERSECURITY: PROTECTING CRITICAL INFRASTRUCTURES FROM CYBER ATTACK AND CYBER WARFARE (Thomas A. Johnson ed., 2015); Tatiana Tropina, *Public-Private Collaboration: Cybercrime, Cybersecurity, and National Security*, *in* SELF- AND CO-REGULATION IN CYBERCRIME, CYBERSECURITY, AND NATIONAL SECURITY 1–42 (2015).

81. Shaun Waterman, *Former DoD Official: U.S. 'More and More Vulnerable' to Cyberattacks*, CYBERSCOOP (June 7, 2017), http://www.cyberscoop.com/former-dod-official-u-s-vulnerable-cyberattacks/ [http://web.archive.org/web/20200421195722/https://www.cyberscoop.com/former-dod-official-u-s-vulnerable-cyberattacks/].

82. Chris Bing, *Microsoft's Chip Patch is Messing with Anti-virus Products*, CYBERSCOOP (Jan. 5, 2018), htt://www.cyberscoop.com/spectre-meltdown-microsoft-anti-virus-bsod/ [https://web.archive.org/web/20200307215245/http://www.cyberscoop.com/spectre-meltdown-microsoft-anti-virus-bsod/]; Michelai Graham, *Report: Criminals Loved to Target PowerPoint in 2017*, CYBERSCOOP (Mar. 27, 2018), http://www.cyberscoop.com/report-cybercriminals-exploited-powerpoint-lot-2017-steal-money-information/ [https://web.archive.org/web/20200307215202/http://www.cyberscoop.com/report-cybercriminals-exploited-powerpoint-lot-2017-steal-money-information/].

has begun to include "information warfare" in its approach to cybersecurity.[83]

A National Security Presidential Directive (NSPD) from 2008 defined cybersecurity as:

> prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.[84]

Seven years later, in the Cybersecurity Act of 2015, Congress defined a cybersecurity threat both more narrowly, by excluding authentication and non-repudiation of information, and more broadly, by including information that is processed by or transiting an information system, not only that which is stored (or contained) thereon:

> an action, not protected by the First Amendment to the Constitution of the United States, on or through an information

---

83. Mark Pomerleau, *Air Force Creates New Information Warfare Organization, Revamps Cyber Command teams*, FIFTH DOMAIN (Sept. 18, 2019), https://www.fifthdomain.com/dod/air-force/2019/09/19/air-force-creates-new-information-warfare-organization-revamps-cyber-command-teams/ [https://web.archive.org/web/20200307215126/https://www.fifthdomain.com/dod/air-force/2019/09/19/air-force-creates-new-information-warfare-organization-revamps-cyber-command-teams/]; Ben Sisario, *Netflix Blocks Show in Saudi Arabia Critical of Saudi Prince*, N.Y. TIMES (Jan. 1, 2019), https://www.nytimes.com/2019/01/01/business/media/netflix-hasan-minhaj-saudi-arabia.html [https://web.archive.org/web/20200307215046/https://www.nytimes.com/2019/01/01/business/media/netflix-hasan-minhaj-saudi-arabia.html]; Shannon Vavra, *Army Cyber Command is Trying to Become an Information Warfare Force*, CYBERSCOOP (Aug. 22, 2019), http://www.cyberscoop.com/cyber-command-information-warfare/ [https://web.archive.org/web/20200307215012/http://www.cyberscoop.com/cyber-command-information-warfare/]; Shaun Waterman, *NATO Expert: Russians Have it Right—It's Information Security Not Cyber*, CYBERSCOOP (Feb. 16, 2017), https://www.cyberscoop.com/nato-expert-russians-information-security-cybersecurity-election-hack-geers/ [http://web.archive.org/web/20200421200613/https://www.cyberscoop.com/nato-expert-russians-information-security-cybersecurity-election-hack-geers/].

84. National Security Presidential Directive/NSPD-54; Homeland Security Presidential Directive/HSPD-23 (Jan. 8, 2008), https://fas.org/irp/offdocs/nspd/nspd-54.pdf [http://web.archive.org/web/20200421200808/https://fas.org/irp/offdocs/nspd/nspd-54.pdf].

> system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.[85]

The law's definition of cyber threat indicators is even more specific about what these threats entail: malicious reconnaissance; methods of defeating security controls or exploiting security vulnerabilities; anomalous activities that indicate a security vulnerability's existence; causation of a user with legitimate access to unwittingly enable the security control's defeat or security vulnerability's exploitation; and malicious cyber command and control of information systems.[86] The law also refers to the potential harm in addition to any actual harm caused by an incident.[87]

Governments across the world largely allow companies to regulate themselves or to engage in co-regulation regimes, resulting in a patchwork of local, national, and international approaches.[88] Prior to the 2000s, the U.S. government and law enforcement involvement came after security systems had failed and crimes had been committed.[89] In 1997, President Bill Clinton issued the U.S. Framework for Global Electronic Commerce that was consistent with the self-regulation approach and, in some ways, set the stage for future emphasis on information sharing rather than heavier government involvement.[90] Principles laid out in the framework included that the private sector should lead, that any government involvement should support and enforce a predictable and minimalist legal environment, and that governments should recognize the ways that the internet is unique from other forms of communication like TV and radio if they decide to pursue regulation; those unique features include the internet's decentralized nature and "bottom-up governance."[91]

---

85. 6 U.S.C. § 1501 (2015).

86. *Id.*

87. *Id.*

88. Cormac Callanan, *Evolution, Implementation, and Practice of Internet Self-regulation, Co-regulation, and Public-Private Collaboration*, *in* SELF- AND CO-REGULATION IN CYBERCRIME, CYBERSECURITY, AND NATIONAL SECURITY 43, 43–100 (2015); Tropina, *supra* note 80.

89. Tropina, *supra* note 80.

90. President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (July 1, 1997) [hereinafter *Framework*], https://fas.org/irp/offdocs/pdd-nec-ec.htm [http://web.archive.org/web/20200421201932/https://fas.org/irp/offdocs/pdd-nec-ec.htm].

91. Callanan, *supra* note 88; *Framework*, *supra* note 90.

In light of the traditionally-light regulatory stance towards the internet and cybersecurity, the U.S. government has advanced information sharing as a policy alternative through both laws and executive orders. This section discusses information sharing within the cybersecurity context and barriers to participation for private actors; state, local, tribal, and territorial (SLTT) governments; and federal agencies.[92]

A. The Development of Cybersecurity Information Sharing Policy

The Senate Homeland Security and Governmental Affairs Committee pursued a classic "softening up" strategy in the 111th and 112th Congresses as it worked toward a comprehensive legislative response to cybersecurity; a 2010 hearing helped define the problem and featured testimony supportive of the committee leaders' approach to the issue, while a hearing two years later saw members of Congress, current and former Homeland Security secretaries, and representatives from think tanks and corporations offer their opinions on the latest iteration of the committee's bill.[93] Homeland Security and Government Affairs Committee chairman Joe Lieberman (D-CT) had decided to retire from the Senate, and the Cybersecurity Act of 2012 (CSA2012) was meant to be his last major legislative achievement.[94] The bill would have established a National Cybersecurity Council, chaired by the Secretary of Homeland Security, that would conduct sector-by-sector risk assessments, identify categories of critical infrastructure, and encourage and coordinate the adoption of voluntary cybersecurity standards.[95] Among other provisions, the bill also would have directed the Department of Homeland Security (DHS) to establish a Critical Infrastructure Cybersecurity Tip Line; required the new Council to develop procedures under which owners of critical cyber infrastructure would be required to report significant incidents; authorized private entities to monitor cybersecurity threats, including threats to a third party

92. *See infra* Part III.A–B.

93. *Critical Infrastructure in the Age of Stuxnet: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 111th Cong. (2010).

94. Lieberman previously led the congressional effort to create the Department of Homeland Security. *See Lieberman Calls for Refocusing Military Resources to Strengthen Homeland Security*, HSGAC.SENATE.GOV (June 26, 2002), https://www.hsgac.senate.gov/media/majority-media/lieberman-calls-for-refocusing-military-resources-to-strengthen-homeland-security [https://web.archive.org/web/20200614053630/https://www.hsgac.senate.gov/media/majority-media/lieberman-calls-for-refocusing-military-resources-to-strengthen-homeland-security].

95. S. 3414, 112th Cong. (2012).

(with that third party's consent); directed the DHS to establish procedures for sharing cybersecurity threat indicators and designate a civilian federal agency as the lead cybersecurity information sharing exchange; and shifted authority for enforcing federal agency information security requirements from the Office of Management and Budget to the DHS.[96] The bill was filibustered once it reached the Senate floor, and the measure died at the end of the 112th Congress.[97]

The Senate Homeland Security and Governmental Affairs Committee maintained its attention on cybersecurity the following year under new chairman Tom Carper (D-DE) but with a narrower focus. The committee's two hearings on cybersecurity in the 113th Congress discussed "strengthening" (really directing) public-private partnerships between the DHS, Department of Commerce, and other executive branch agencies and internet security firms to address the issue absent the force of law.[98] Two bills were introduced that term: the Cyber Intelligence Sharing and Protection Act in the House, and the Cybersecurity Information Sharing Act. The former would have required the Director of National Intelligence to establish procedures that would encourage the intelligence community to share cyber threat information with utilities and other private entities and that would allow non-governmental cybersecurity services providers to obtain and share (with third-party consent) cyber threat information with other private entities and the federal government;[99] the latter eventually became the Cybersecurity Act of 2015.[100]

In 2018, Congress enacted the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act, which directed the DHS to develop a vulnerability disclosure policy and report on its progress annually to Congress.[101] The law also required the executive branch to develop an information sharing program for

---

96. *Id.* Lieberman introduced an earlier bill, S. 2105, also called the Cybersecurity Act of 2012, but that bill did not advance past committee.

97. The bill received fifty-one votes, nine votes shy of the sixty votes needed, to agree to a motion to invoke cloture and reduce debate time on the bill.

98. *Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. (2014); *The Cybersecurity Partnership Between the Private Sector and our Government: Protecting our National and Economic Security: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. (2013).

99. Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2011).

100. Jonathan Meyer & Amber C. Thomson, *The Cybersecurity Act of 2015*, CLOUD COMPUTING LEGAL DESKBOOK § 4:9 (2018).

101. Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Pub. L. No. 115-390. 132 Stat. 5173 (2018).

cybersecurity risks to the federal acquisition supply chain.[102] The renewed emphasis on information sharing likely stems from the connections and similarities between cybersecurity and homeland security. Policymakers typically face a "deliberation-preparation tradeoff": they can either deliberate over and develop the most appropriate alternative for a given problem, which hampers timely responses, or they can economize on time and use a previously-prepared alternative that may not be the best fit for the specific problem at hand.[103] Policymakers further "reason by analogy" and borrow ideas from other policy areas that share some similar characteristics.[104] In the absence of more comprehensive cybersecurity legislation, Congress turned to an idea already "available" in a policy area that overlaps with cybersecurity in some of its attributes, and in the agencies to which information gathering and coordinating authority already had been delegated.

In its report, the 9/11 Commission identified that the U.S. government had access to a lot of information but lacked adequate capacity to process and use that information. As the 9/11 Commission wrote, "Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information . . . There are no punishments for *not* sharing information. Agencies uphold a 'need to know' culture of information protection rather than promoting a 'need to share' culture of integration."[105] The Critical Infrastructure Information Act of 2002, enacted as part of the Homeland Security Act of 2002, authorized the DHS to foster the voluntary transmission of information about threats to critical infrastructure from private entities to federal agencies through the Protected Critical Infrastructure Information Program.[106] The Intelligence Reform and Terrorism Prevention Act of 2004 created the Office of the Director of National Intelligence in part to address the Commission's finding and to integrate intelligence-related information gathered across multiple agencies.[107] Think tanks and academics began arguing for a

---

102. *Id.*

103. BRYAN D. JONES, POLITICS AND THE ARCHITECTURE OF CHOICE: BOUNDED RATIONALITY AND GOVERNANCE (2001).

104. Anne Schneider & Helen Ingram, *Systematically Pinching Ideas: A Comparative Approach to Policy Design*, 8 J. PUB. POL'Y 61, 61–80 (1988); Jack L. Walker, *The Diffusion of Innovations Among the American States*, 63 AM. POL. SCI. REV. 880, 880–99 (1969).

105. *9/11 Report*, *supra* note 5, at 417.

106. Critical Infrastructure Act of 2002, Pub. L. No. 107-296, tit. II, § 214, 116 Stat. 2152 (codified as amended 6 U.S.C. § 673 (2018)).

107. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, tit. I, § 1011(a), 118 Stat. 3644 (codified as amended 50 U.S.C. § 3023 (2018)).

larger private-sector role in homeland security in light of the use of commercial aviation in the September 11, 2001 terrorist attack; and the private sector aid response to Hurricane Katrina in 2005; and controversy over the Dubai Ports World acquisition of management contracts for six U.S. ports.[108]

The executive branch also has encouraged information sharing as part of a broader cybersecurity strategy though its interest in cybersecurity has largely concerned critical infrastructure protection. In 2004, President George W. Bush issued the classified NSPD 38 which laid out a National Strategy to Secure Cyberspace, and, four years later, the NSPD 54 directed agencies to increase their efforts to coordinate and enhance the security of their own networks and those of critical infrastructure sectors.[109] Upon taking office, President Barack Obama ordered a review of U.S. cybersecurity efforts and the resulting Cyberspace Policy Review initiatives included an expanded, government-wide cyber counterintelligence plan and developing a plan of shared action between the DHS and private sector actors to more clearly define the federal government's role in extending its cybersecurity into critical infrastructure sectors.[110] Obama's Executive Order 13636 cited "repeated cyber intrusions into critical infrastructure" as justification for improved cybersecurity policies and stated that U.S. policy would be "to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities."[111] President Donald Trump's Executive Order 13800 represents a broader approach to cybersecurity in government, including reporting requirements for agencies on efforts to educate and train a cybersecurity workforce, but

---

108. Daniel B. Prieto, *Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects*, *in* SEEDS OF DISASTER, ROOTS OF RESPONSE: HOW PRIVATE ACTION CAN REDUCE PUBLIC VULNERABILITY (Philip E. Auerswald et al. eds., Cambridge Univ. Press 2006); STEPHEN E. FLYNN & DANIEL B. PRIETO, *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security*, BELFER CTR. (Mar. 2006), https://www.belfercenter.org/publication/neglected-defense-mobilizing-private-sector-support-homeland-security [https://web.archive.org/web/20200614065448/https://www.belfercenter.org/publication/neglected-defense-mobilizing-private-sector-support-homeland-security].

109. WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2004); *see also National Security Presidential Directive/NSPD-54*, *supra* note 84.

110. JOHN ROLLINS & ANNA C. HENNING, CONG. RESEARCH SERV., R40427, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS (2009), https://fas.org/sgp/crs/natsec/R40427.pdf [http://web.archive.org/web/20200424215535/https://fas.org/sgp/crs/natsec/R40427.pdf].

111. Exec. Order No. 13,636, 78 Fed. Reg. 11,737 (2013).

still emphasizes critical infrastructure cybersecurity protection as U.S. executive branch policy.[112]

In both legislative and executive action, the cybersecurity information being shared refers to the transmission of information about vulnerabilities and threats.[113] Those vulnerabilities might arise from older technology and software that lacks protection from more current methods of intrusion or attack;[114] newer software that has not been adequately tested;[115] and human behaviors such as clicking on malicious links in emails or using compromised technology.[116] Data breaches, one type of cybersecurity vulnerability, may even occur when government agencies share the wrong data with each other.[117] When information about threats and vulnerabilities is shared, it may carry secondary information about which groups are responsible for the threat.[118] Information sharing as a

112. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (2017).

113. *Id.*

114. Lily Hay Newman, *Decades-Old Code Is Putting Millions of Critical Devices at Risk*, WIRED (Oct. 1, 2019, 11:12 AM), https:/www.wired.com/story/urgent-11-ipnet-vulnerable-devices/?wpisrc=nl_cybersecurity202&wpmm=1 [http://web.archive.org/web/20200307034819/https:/www.wired.com/story/urgent-11-ipnet-vulnerable-devices/?wpisrc=nl_cybersecurity202&wpmm=1].

115. Bing, *supra* note 82.

116. Chris Bing, *Hacker Breaches Navy, Compromises Records of More Than 130,000 Sailors*, CYBERSCOOP (Nov. 28, 2016), https:/www.cyberscoop.com/hacker-breaches-navy-compromises-records-130000-sailors/ [http://web.archive.org/web/20200307034724/https:/www.cyberscoop.com/hacker-breaches-navy-compromises-records-130000-sailors/]; Jack Stubbs et al., *Inside the West's Failed Fight Against China's "Cloud Hopper" Hackers*, REUTERS (June 26, 2019, 6:00 AM), https:/www.reuters.com/investigates/special-report/china-cyber-cloudhopper/ [http://web.archive.org/web/20200307034640/https:/www.reuters.com/investigates/special-report/china-cyber-cloudhopper/]; Morgan Theophil, *Commissioners Move to Update Victoria County's Cybersecurity Policy*, VICTORIA ADVOCATE (Jan. 13, 2020), https://www.victoriaadvocate.com/news/government/commissioners-move-to-update-victoria-county-s-cybersecurity-policy/article_894f7f7a-361a-11ea-afba-bf4a2e4a8239.html [http://web.archive.org/web/20200421203402/https://www.victoriaadvocate.com/news/government/commissioners-move-to-update-victoria-county-s-cybersecurity-policy/article_894f7f7a-361a-11ea-afba-bf4a2e4a8239.html].

117. Ryan Johnston, *California DMV Data Breach Shared Social Security Information of Thousands*, STATESCOOP (Nov. 6, 2019), http://statescoop.com/california-dmv-data-breach-shared-social-security-information-of-thousands/ [http://web.archive.org/web/20200307034359/http://statescoop.com/california-dmv-data-breach-shared-social-security-information-of-thousands/].

118. Shannon Vavra, *Cyber Command's Latest Virus Total Upload Has Been Linked to an Active Attack*, CYBERSCOOP (May 21, 2019), https:/www.cyberscoop.com/cyber-command-virustotal-apt28-kaspersky-zonealarm/ [http://web.archive.org/web/20200307032912/https:/www.cyberscoop.com/cyber-command-virustotal-apt28-kaspersky-zonealarm/] [hereinafter *Cyber Command's Latest*

policy alternative is based on the idea that if agencies and companies are aware of where and how they are vulnerable, they can take the necessary steps to mitigate those vulnerabilities before they experience a cyberattack. Some vulnerabilities are considered so urgent they are called "zero days," in that the manufacturer or company has "zero days" to fix the security flaw.[119] Government agencies share cybersecurity threat and vulnerability information in several ways, including official Vulnerability Equities Process and Automated Indicator Sharing programs and by using privately-owned platforms like VirusTotal that aggregate information about malware, viruses, and other threats not covered by existing software.[120] The DHS has established cybersecurity Information Sharing and Analysis Centers around the country as well as a Cyber Information Sharing and Collaboration Program, and, in 2018, Congress reorganized the DHS to replace the National Protection and Programs Directorate with the Cybersecurity and Infrastructure Security Agency, in part to ensure that information sharing would be a priority within homeland security.[121] Worth noting here is that authority for coordinating information sharing in the Cybersecurity Act of 2015 (CSA) is largely placed with the federal defense, intelligence, homeland security, and law enforcement agencies in line with Obama's actions but in contrast with Lieberman's 2012 CSA, which would have directed

---

Virus Total Upload]; Shannon Vavra, *U.S. Cyber Command Warns of North Korea-linked Lazarus Group Malware*, CYBERSCOOP (Aug. 15, 2019), https:/www.cyberscoop.com/lazarus-group-hacking-malware-cyber-command/ [http://web.archive.org/web/20200307032747/https:/www.cyberscoop.com/lazarus-group-hacking-malware-cyber-command/] [hereinafter *U.S. Cyber Command Warns of North Korea-linked Lazarus Group Malware*].

119. Shaun Waterman, *Zero-day study: Hoarding exploits less harmful than generally thought*, SCOOP NEWS GROUP (Mar. 9, 2017), https:/www.cyberscoop.com/study-hoarded-zero-days-last-seven-years-and-are-rarely-discovered/ [http://web.archive.org/web/20200307032310/https:/www.cyberscoop.com/study-hoarded-zero-days-last-seven-years-and-are-rarely-discovered/].

120. Greg Otto, *White House Unveils Process Behind Disclosing Software Vulnerabilities*, CYBERSCOOP (Nov. 15, 2017), https:/www.cyberscoop.com/vulnerabilities-equities-process-vep-charter-white-house-rob-joyce/ [http://web.archive.org/web/20200307032618/https:/www.cyberscoop.com/vulnerabilities-equities-process-vep-charter-white-house-rob-joyce/]; *Cyber Command's Latest Virus Total Upload*, *supra* note 118.

121. Mark Rockwell, *DHS Cyber Re-Org Clears Congress*, FCW (Nov. 14, 2018), https://fcw.com/articles/2018/11/14/cisa-not-nppd-bill-rockwell.aspx [http://web.archive.org/web/20200421203642/https://fcw.com/articles/2018/11/14/cisa-not-nppd-bill-rockwell.aspx].

DHS to designate a civilian agency to serve as the lead information sharing exchange.[122]

From the preceding discussion, we can understand the Cybersecurity Act of 2015 and reliance on information sharing as a policy alternative within cybersecurity as the product of four dynamics: first, the tradition of Internet self-governance and the prevailing idea that the government should encourage a minimalist legal environment over the Internet; second, Congress's inability to pass broader, more comprehensive cybersecurity laws; third, the availability of "information sharing" as an alternative in a related issue area; and fourth, the executive branch's allocation of authority over cybersecurity policy to defense, intelligence, homeland security, and law enforcement agencies. These dynamics help produce challenges to congressional oversight. Whereas information about drug trafficking, for example, is largely shared between federal, state, and local governments, cybersecurity information sharing involves privately-owned entities and changes in the nature of the threats and vulnerabilities that may not be known until they are discovered.

Three types of actors might share information about cybersecurity threats and vulnerabilities: private companies, SLTT governments, and federal agencies.[123] Each of these actors also has reasons why it may not share relevant information that can create barriers to effective congressional oversight and policy effectiveness as described in the remainder of this section.[124]

B. Barriers to Participation in Cybersecurity Information Sharing

Despite the multiple executive orders in the 2000s and the 2015 law, as of 2018, only six private entities were sharing information with the Department of Homeland Security's Automated Indicator Sharing program.[125] Private-sector information sharing programs have lagged

---

122. Cybersecurity Act of 2015, Pub. L. No. 114-113, Div. N, tit. I, 129 Stat. 2935, (current version at 6 U.S.C. §§ 1501–10 (2018)); Cybersecurity Act of 2012, S. 2105, 114th Cong. (2014).

123. DEPARTMENT OF HOMELAND SECURITY, A GUIDE TO CRITICAL INFRASTRUCTURE AND KEY RESOURCES PROTECTION AT THE STATE, REGIONAL, LOCAL, TRIBAL, AND TERRITORIAL LEVEL (2008), https://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf [http://web.archive.org/web/20200322210556/https://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf].

124. *See infra* Part III.B.

125. Chris Bing, *Ransomware Attacks Are Rarely Being Reported to The FBI, New Data Shows*, CYBERSCOOP (June 22, 2017), https:/www.cyberscoop.com/ransomware-fbi-ic3-2016-report/ [http://web.archive.org/web/20200307032018/https:/www.cyberscoop.com/ransomware-fbi-ic3-2016-report/]; Joseph Marks, *Only 6 Non-Federal Groups Share Cyber Threat*

largely because businesses do not feel participation is in their interests. Three interrelated reasons help explain the lack of incentive. First is that many businesses believe they gain a competitive advantage from keeping information about threats and vulnerabilities to themselves.[126] If a company recognizes a sector-wide vulnerability, it might quietly protect itself and leave its competitors to remain vulnerable. Companies may also worry that sharing information about vulnerabilities would reveal to their competitors proprietary information about their operations and business practices.[127] Conversely, protection from cybersecurity threats and vulnerabilities might be considered a collective good, which then experiences free rider problems; a company might let its competitors or the government invest the resources required to discover and share information about vulnerabilities and then integrate whatever information others produce.[128]

The second factor working against business participation in cybersecurity information sharing is a concern over reputation and liability. The Cybersecurity Act of 2015 prevents companies from being held liable for simply sharing information about threats and vulnerabilities, but companies remain liable for any damage, data loss, or other consequences of actual cyberattacks and data breaches.[129] A cybersecurity insurance industry has developed over the past decade, but

---

Info with Homeland Security, NEXTGOV (June 27, 2018), http:/www.nextgov.com/cybersecurity/2018/06/only-6-non-federal-groups-share-cyber-threat-info-homeland-security/149343/ [http://web.archive.org/web/20200307031329/http:/www.nextgov.com/cybersecurity/2018/06/only-6-non-federal-groups-share-cyber-threat-info-homeland-security/149343/].

126. Sean Lyngaas, *Hoarding Threat Information "Not a Competitive Advantage," DHS Official Tells Corporate Leaders*, CYBERSCOOP (Dec. 5, 2018), https:/www.cyberscoop.com/hoarding-threat-information-not-competitive-advantage-dhs-official-tells-corporate-leaders/ [http://web.archive.org/web/20200307031829/https:/www.cyberscoop.com/hoarding-threat-information-not-competitive-advantage-dhs-official-tells-corporate-leaders/]; Shaun Waterman, *Cyber Companies Urged to Share—and Not Sell—Threat Info*, CYBERSCOOP (Sept. 11, 2017), https:/www.cyberscoop.com/threat-intelligence-sharing-insa-john-felker/ [http://web.archive.org/web/20200307031659/https:/www.cyberscoop.com/threat-intelligence-sharing-insa-john-felker/]; *Zero-day Study*, *supra* note 119.

127. Sean Lyngaas, *Misconceptions Hinder Threat-Sharing with Government, DHS Official Says*, CYBERSCOOP (Nov. 14, 2019), https:/www.cyberscoop.com/threat-intelligence-sharing-insa-john-felker/ [http://web.archive.org/web/20200307031659/https:/www.cyberscoop.com/threat-intelligence-sharing-insa-john-felker/].

128. Marks, *supra* note 125.

129. 6 U.S.C. § 1505(c) (2018) ("Nothing in this subchapter shall be construed . . . to undermine or limit the availability of otherwise applicable common law or statutory defenses.").

insurance providers have been reluctant to pay claims and some have reconsidered engaging with the cybersecurity market entirely.[130] Companies may wait until they have patched or otherwise repaired a vulnerability before they report it, which also may take place after users unknowingly have experienced attacks. Even if companies do patch vulnerable software or equipment, doing so may void a warranty and leave them financially responsible for any future repairs and updates.[131]

Third, companies may not participate in information sharing exchanges because they do not value the information they receive from the government. Initial efforts by the DHS and other agencies to share threat information with the private sector focused on volumes of technical information, and the information the government shares may not be timely (in part for reasons discussed below); companies, for their part, place greater value on context and fear "false positives" that could lead them to expend cybersecurity resources in the wrong areas.[132]

State, local, tribal, and territorial (SLTT) governments typically receive information about cybersecurity threats and vulnerabilities more

---

130. Jeff Stone, *Demand for Cyber Insurance Grows as Volatility Scares Off Some Providers*, CYBERSCOOP (July 29, 2019), https:/www.cyberscoop.com/cyber-insurance-demand-cost-2019/ [http://web.archive.org/save/https:/www.cyberscoop.com/cyber-insurance-demand-cost-2019/]; Jeff Stone, *AIG Must Cover Client's $5.9 Million in Cyber-related Losses, Judge Rules*, CYBERSCOOP (Jan. 31, 2020), https://www.cyberscoop.com/aig-cyber-insurance-ssc-technologies/ [http://web.archive.org/web/20200421204219/https://www.cyberscoop.com/aig-cyber-insurance-ssc-technologies/].

131. Ellen Sundra, *Cybersecurity's Warranty Challenge*, CYBERSCOOP (Jan. 7, 2020), https:/www.cyberscoop.com/cybersecurity-patching-versus-warranty-ellen-sundra-forescout/ [http://web.archive.org/web/20200307030928/https:/www.cyberscoop.com/cybersecurity-patching-versus-warranty-ellen-sundra-forescout/].

132. Cory Bennett, *What Our Cyberwall Knows*, POLITICO (Oct. 11, 2017, 5:04 AM), https:/www.politico.com/agenda/story/2017/10/11/government-cyber-attack-companies-000539?lo=ap_b1 [http://web.archive.org/web/20200307030828/https:/www.politico.com/agenda/story/2017/10/11/government-cyber-attack-companies-000539?lo=ap_b1]; Jeff Stone, *Mistrust Lingers Between Government, Industry on Cyber Information Sharing*, CYBERSCOOP (Oct. 24, 2019), https:/www.cyberscoop.com/cyber-information-sharing-dhs-uber/ [http://web.archive.org/web/20200307030750/https:/www.cyberscoop.com/cyber-information-sharing-dhs-uber/] [hereinafter *Mistrust Lingers*]; Shannon Vavra, *The NSA Recognizes It Needs to Share More Nation-state Threat Data, and faster*, CYBERSCOOP (Sept. 5, 2019), https:/www.cyberscoop.com/nsa-threat-data-info-sharing-cybersecurity-directorate/ [http://web.archive.org/web/20200307030718/https:/www.cyberscoop.com/nsa-threat-data-info-sharing-cybersecurity-directorate/]; *Understanding Cybersecurity Threats to America's Aviation Sector: Hearing Before the H. Subcomms. on Cybersecurity & Infrastructure Prot. and Transp. & Prot. Sec. of the H. Comm. on Homeland Sec.*, 115th Cong. (2018) (statement of the Comm. of Homeland Security).

so than they share information, but, like private companies, they may fear any hit to their reputation that comes from revealing any threats or attacks they have experienced. SLTT government budgets also are much smaller than those of the federal government and some major companies, giving them fewer resources to spend on cybersecurity and lower capacity to detect and understand threats and vulnerabilities.[133]

For federal agencies, perhaps the most significant barrier to more effective information sharing is the nature of the threats themselves. Threats and attacks involving actors based in other countries, whether affiliated with nation-states or not, and threats involving industries and resources designated as critical infrastructure involve national and homeland security and, thus, some degree of classified information. The de-classification process is understandably cautious and involves multiple gatekeepers, which then delays the information getting to those who may need it.[134] As with companies, agencies may view both the information and the process by which they acquired that information to be proprietary. Agencies responsible for monitoring and detecting threats may compete to claim credit, which then changes their willingness to share those threats. For other agencies, sharing information about vulnerabilities, particularly data breaches, brings public and

---

133. Benjamin Freed, *Cleveland Officials Plead Ignorance on Airport Ransomware Incident, Local Media Unimpressed*, STATESCOOP (Apr. 30, 2019), https:/statescoop.com/cleveland-officials-plead-ignorance-on-airport-ransomware-incident-local-media-unimpressed/ [http://web.archive.org/web/20200307030617/https:/statescoop.com/cleveland-officials-plead-ignorance-on-airport-ransomware-incident-local-media-unimpressed/]; Jake Williams, *Iowa Offers a Model to Kickstart Cyberthreat Info Sharing in Counties*, STATESCOOP (Feb. 19, 2016), https:/statescoop.com/iowa-offers-a-model-to-kickstart-cyberthreat-info-sharing-in-counties/ [http://web.archive.org/web/20200307030504/https:/statescoop.com/iowa-offers-a-model-to-kickstart-cyberthreat-info-sharing-in-counties/]; Colin Wood, *States Name Three Ways Feds Can Help with Cybersecurity*, STATESCOOP (Jan. 22, 2020), https://statescoop.com/nascio-federal-advocacy-priorities-2020-gao-omb-cybersecurity/ [http://web.archive.org/web/20200421204546/https://statescoop.com/nascio-federal-advocacy-priorities-2020-gao-omb-cybersecurity/].

134. Chris Bing, *Why Businesses Ignore the U.S. Government's Information Sharing Programs*, CYBERSCOOP (Jan. 31, 2017), https://www.cyberscoop.com/information-sharing-cybersecurity-dhs-private-sector/ [http://web.archive.org/web/20200421204624/https://www.cyberscoop.com/information-sharing-cybersecurity-dhs-private-sector/]; Shannon Vavra, *NSA: "We Know We Need to Do Some Work" on Declassifying Threat Intel*, CYBERSCOOP (Oct. 24, 2019), https://www.cyberscoop.com/anne-neuberger-nsa-threat-intelligence-cyber-talks-2019/ [http://web.archive.org/web/20200322221905/https://www.cyberscoop.com/anne-neuberger-nsa-threat-intelligence-cyber-talks-2019/] [hereinafter *We Know We Need to Do Some Work*]; Bennett, *supra* note 132.

congressional scrutiny and, perhaps, financial responsibility for remedying the breaches.[135] Another significant barrier to federal government information sharing may be a lack of capacity to adequately detect and share information. Government positions tend to pay less than the private sector positions, and so the most talented cybersecurity experts may not pursue or stay in agency positions.[136] Even for those in government, the nature of cybersecurity threats changes quickly and may move beyond an individual's expertise.[137]

One additional barrier to information sharing exists for all three actors: the nature of cybersecurity as a policy problem itself. One similarity to homeland security generally is that cybersecurity is something to be managed rather than something that can be completely solved; it involves the language of risk and resilience rather than the language of prevention. Cybersecurity is often evaluated based on government or company responses to vulnerabilities, threats, and incidents rather than the incidents themselves.[138] Information thus may not be shared until after a threat or vulnerability has been discovered and remedied or after an incident has occurred; knowing that a vulnerability exists may be less important than knowing what to do about it.

While the preceding discussion also indicates some ways in which cybersecurity generally poses challenges to policymaking, this Article

---

135. Chris Bing, *OPM Hearing Devolves into Shouting Match About Cybersecurity*, CYBERSCOOP (Feb. 2, 2017), https://www.cyberscoop.com/opm-cybersecurity-russian-hacking-stephen-lynch-jason-chaffetz/ [http://web.archive.org/web/20200421204720/https://www.cyberscoop.com/opm-cybersecurity-russian-hacking-stephen-lynch-jason-chaffetz/]; Chris Bing, *After 2015 Breach, OPM Overpaid for Identity Theft Protections, Report Finds*, CYBERSCOOP (Mar. 31, 2017), https://www.cyberscoop.com/2015-breach-opm-overpaid-identify-theft-protections-report-finds/ [http://web.archive.org/web/20200421204800/https://www.cyberscoop.com/2015-breach-opm-overpaid-identify-theft-protections-report-finds/].

136. *See* Ellen Nakashima, *Federal Agencies, Private Firms Fiercely Compete in Hiring Cyber Experts*, WASH. POST (Nov. 13, 2012), https://www.washingtonpost.com/world/national-security/federal-agencies-private-firms-fiercely-compete-in-hiring-cyber-experts/2012/11/12/a1fb1806-2504-11e2-ba29-238a6ac36a08_story.html [https://web.archive.org/web/20200614083514/https://www.washingtonpost.com/world/national-security/federal-agencies-private-firms-fiercely-compete-in-hiring-cyber-experts/2012/11/12/a1fb1806-2504-11e2-ba29-238a6ac36a08_story.html].

137. Bennett, *supra* note 132.

138. Jake Williams, *Cities and Their Residents Need "Honest Conversation" on Cybersecurity*, STATESCOOP (Nov. 19, 2019), https://statescoop.com/cities-honest-conversation-cybersecurity-barcelona-expo-world-congress/ [http://web.archive.org/web/20200421204837/https://statescoop.com/cities-honest-conversation-cybersecurity-barcelona-expo-world-congress/]; Todt, *supra* note 4.

specifically focuses on congressional oversight of information sharing. As described above, "information sharing" has some unique features that differentiate it from other forms policy alternatives like taxes and regulations. Information sharing, thus, does not fit neatly within our existing frameworks for understanding how Congress conducts effective oversight. The next section discusses some of the more general challenges to congressional oversight that cybersecurity information sharing poses, then it traces back through the individual oversight tools described earlier in the Article.[139]

IV. CHALLENGES FOR EFFECTIVE CONGRESSIONAL OVERSIGHT

Members of Congress value position-taking and credit-claiming opportunities, and legislative activity and constituent service tend to provide those opportunities to a greater degree than oversight; legislative action tends to be more visible than all but the highest-profile oversight hearings.[140] To the extent that oversight provides clear position-taking opportunities, it does so when either district, state, or party interests are involved. Cybersecurity information sharing may be a case where the lack of a clear partisan dimension hinders the prospects for effective oversight; members of the presidential out-party lack obvious incentives to elevate attention to information sharing by embarrassing the current administration.

Another challenge is not necessarily unique to cybersecurity information sharing: how to measure whether oversight activities were successful. The stated congressional policy (as expressed through law) is for agencies to coordinate information exchange about cybersecurity threats with SLTT governments and the private sector. Sharing *more* information cannot be the end goal because too much information can actually be less helpful.[141] Cybersecurity threats change over time and, thus, so will the specific information about those threats that would need to be shared, which in turn changes some of the appropriate metrics of "success." Is sharing the information alone enough to consider the policy successful, or does that information also have to be timely and acted upon?

---

139. *See infra* Part IV.

140. *See* JONATHAN LEWALLEN, COMMITTEES AND THE DECLINE OF LAWMAKING IN CONGRESS (Univ. of Mich. Press 2020) (discussing how changes to congressional rules and practices since the 1970s have made legislating a less-attractive prospect for committees); DAVID R. MAYHEW, CONGRESS: THE ELECTORAL CONNECTION (Yale Univ. Press 1974); Seymour Scher, *Conditions for Legislative Control*, 25 THE J. OF POLITICS, 526, 526–51 (1963).

141. Bennett, *supra* note 132; *Mistrust Lingers*, *supra* note 132.

One general oversight challenge is specific to information sharing: the information related to cybersecurity threats and vulnerabilities is to flow between agencies, SLTT governments, and the private sector without also flowing to Congress. Legislators already face an information disadvantage relative to the bureaucracy; bureaucrats know more about the policy problems and likely effects of proposed alternatives to a greater degree.[142] That disadvantage may be exacerbated with cybersecurity information sharing: Congress does not know what information agencies and companies *could be* but *are not* sharing. And whereas Congress can rely on constituents, interest groups, and other "fire alarms" to help reduce its information asymmetry for other policies,[143] almost by definition these groups do not know what information agencies are not sharing, either. Conversely, the problem definition and uncertainty reduction functions that bureaucracies perform for Congress may suffer because agencies also do not know what threat or vulnerability information the private sector is not sharing. Congress finds itself in a position of promotion—"what can we do to help?"—without knowing what kind of information would be shared with more resources, incentives, and support. And while oversight does not necessarily have to be adversarial, that advocacy position creates a conundrum: Congress can provide positive incentives for participation or improvement but fewer sanctions for non-participation.

Overlapping agency responsibility for cybersecurity generally and information sharing specifically poses another challenge to effective congressional oversight. Multiple agencies may share information about the same cyber vulnerabilities and threats, which then creates confusion about responsibility for both the private sector and for Congress.[144] The Department of Health and Human Services played a significant role in notifying the U.S. health care sector about the 2018 "WannaCry" ransomware attack on entities and industries around the world (including the British National Health Service), but some legislators looked to the DHS and Office of Management and Budget for a response in the attack's aftermath.[145] Overlapping responsibility may also manifest when

142. Scher, *supra* note 140.

143. Barry R. Weingast, *The Congressional-Bureaucratic System: A Principal-Agent Perspective (with Applications to the SEC)*, 44 PUB. CHOICE 147–91 (1984); McCubbins & Schwartz, *supra* note 38.

144. *We Know We Need to Do Some Work*, *supra* note 134.

145. Shaun Waterman, *Sen. Warner Wants Action on WannaCry Patching from DHS, OMB*, CYBERSCOOP (May 15, 2017), https://www.cyberscoop.com/sen-warner-wants-action-wannacry-patching-dhs-omb/ [http://web.archive.org/web/20200322223750/https://www.cyberscoop.com/sen-warner-wants-action-wannacry-patching-dhs-omb/]; Shaun Waterman, *WannaCry Outbreak Was*

agencies share information with, or receive information from, an industry outside its traditional substantive jurisdiction, as when the Department of Homeland Security shares vulnerability information about healthcare devices or when the Department of Defense Cyber Command works with the banking sector.[146] Changing technology can make new industries vulnerable and require information sharing in a new domain; the U.S. Farm Credit Administration, for example, recently moved to "cloud computing" and, thus, created new data and system vulnerabilities relevant to cybersecurity information sharing policies and introduced agriculture policy concerns into the cybersecurity domain.[147]

Overlap in agency responsibility and issue involvement raises questions about who in Congress is responsible for conducting oversight; in the Farm Credit Administration case, would it be the homeland security or the agriculture committees? Both have some claim to jurisdiction, and the resulting competition and turf battles among committees can send conflicting signals to agencies about congressional directives.[148] Legislative turf battles, then, can lead to more agency overlap as committees advocate for the agencies under their jurisdiction to gain authority over cybersecurity information sharing, which in turn

---

First Big Test of HHS's New Cybersecurity Center for Health Sector, CYBERSCOOP (June 8, 2017), https://www.cyberscoop.com/wannacry-outbreak-first-big-test-hhss-new-cybersecurity-center-health-sector/ [http://web.archive.org/web/20200322223906/https://www.cyberscoop.com/wannacry-outbreak-first-big-test-hhss-new-cybersecurity-center-health-sector/].

146. Chris Bing, *Inside "Project Indigo," The Quiet Info-sharing Program Between Banks and U.S. Cyber Command*, CYBERSCOOP (May 21, 2018), https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/ [http://web.archive.org/save/https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/] [hereinafter *Inside Project Indigo*]; Jeff Stone, *DHS Pushes Alert on Vulnerable Patient Monitors Sold by GE Healthcare*, CYBERSCOOP (Jan. 23, 2020), https://www.cyberscoop.com/ge-healthcare-dhs-alert/ [http://web.archive.org/web/20200322224129/https://www.cyberscoop.com/ge-healthcare-dhs-alert/]; Shannon Vavra, *Why Cyber Command's Latest Warning Is a Win for the Government's Information Sharing Efforts*, CYBERSCOOP (July 10, 2019), https://www.cyberscoop.com/cyber-command-information-sharing-virustotal-iran-russia/ [http://web.archive.org/web/20200322224256/https://www.cyberscoop.com/cyber-command-information-sharing-virustotal-iran-russia/].

147. Mark Rockwell, *Farm Credit Agency Looks to Cloud*, FWC (Jan. 7, 2020), https://fcw.com/articles/2020/01/07/farm-credit-cloud-rockwell.aspx [http://web.archive.org/web/20200322224716/https://fcw.com/articles/2020/01/07/farm-credit-cloud-rockwell.aspx].

148. Joshua D. Clinton et al., *Influencing the Bureaucracy: The Irony of Congressional Oversight*, 58 AM. J. POL. SCI. 387, 387–401 (2014); Sean Gailmard, *Multiple Principals and Oversight of Bureaucratic Policy-Making*, 21 J. THEORETICAL POL. 161, 161–86 (2009).

would give those committees more policymaking authority in the future.[149]

A. Hearings

Hearings can be an effective oversight tool for reducing Congress's information asymmetry, learning about how current policies are affecting —and prospective policies would affect—constituents and directing bureaucratic attention towards a legislator's preferred issues.[150] The effectiveness of a hearing tends to depend on two factors: sustained attention and the possibility of future legislation.[151] Regarding the former, both individuals and institutions face limits on their attention, and neither allocate attention proportional to the urgency or scope of a problem.[152] The committee system helps Congress, as an institution, pay attention to multiple issues at once, and subcommittees do the same within committees, but paying attention to one issue means shifting attention away from others. Cybersecurity as a policy issue encompasses many component issues, including the privacy of medical records, online money laundering, and international terrorism. These issues involve multiple committees and agencies across jurisdictional boundaries, all of which are engaged in issues besides cybersecurity. Cybersecurity competes for attention within each committee's jurisdiction; a committee with jurisdiction over health policy, for example, must decide at any given point whether it wants to focus on electronic medical records, insurance coverage and cost, government health promotion activities, or another issue. Hearings through 2014 at which cybersecurity was discussed represent about 2.5 percent of hearings related to its different component issues (health, homeland security, technology, etc.); even within congressional hearings related to technology issues through 2014, cybersecurity represents less than ten percent of committee attention.[153] At the same time, information sharing is just one aspect of cybersecurity policy and competes for attention with other concerns; when a committee

149. *Inside Project Indigo*, *supra* note 146.

150. Daniel Diermeier & Timothy J. Feddersen, *Information and Congressional Hearings*, 44 AM. J. POL. SCI. 51–65 (2000).

151. ABERBACH, *supra* note 36; FOREMAN, *supra* note 32.

152. Bryan D. Jones, *Bounded Rationality and Public Policy: Herbert A. Simon and the Decisional Foundation of Collective Choice*, 35 POL'Y SCI. 269, 269–84 (2002); Samuel Workman et al., *Information Processing and Policy Dynamics*, 37 POL'Y STUD. J. 75, 75–92 (2009).

153. Jonathan Lewallen, Assistant Professor, Univ. of Tampa, Presentation at the Southern Political Science Association Annual Meeting: The Attention Dynamics of Cybersecurity in the U.S. Congress (Jan. 11, 2020) (on file with author).

wants to discuss cybersecurity, information sharing may not be the immediate priority. Limits on attention and the array of cybersecurity-related issues on which committees *could* hold hearings, in addition to the other issues over which those committees hold jurisdiction, render the likelihood of sustained attention to cybersecurity information sharing relatively low; oversight becomes "underprovided."[154]

Regarding the possibility (or threat) of future legislative action, the previous section described how information sharing became law in part because Congress could not agree on a more comprehensive approach to cybersecurity. The 2015 law also passed as part of a larger omnibus spending package; legislators tend to vote on omnibus bills based on their support for the overall package, and they are less aware of the specific details contained in the bill.[155] Whether Congress would be able to enact a law reinforcing their oversight findings on cybersecurity information sharing, thus, remains somewhat of an open question. Moreover, the problems experienced thus far—lack of private-sector participation and slow or ineffective information sharing by agencies—are not easily addressed through legislation. The House Committee on Homeland Security recently advanced a bill introduced by Rep. Jim Langevin (D-RI) that would allow the DHS Cybersecurity and Infrastructure Security Agency (CISA) to subpoena internet service providers for information about an information system when CISA finds evidence of a specific vulnerability related to critical infrastructure but cannot identify the information system's owner.[156] That bill and similar approaches delegate even further, rather than enhance, Congress's own authority by giving the executive branch more legal power and by shifting conflict over the exercise of that power to the courts.[157]

B. Investigations

Thorough, effective congressional investigations can take years to complete, and so they need to be worth the time spent.[158] That time required to complete an investigation is likely the biggest challenge to its use as an oversight tool in cybersecurity information sharing.[159] The pace of technological change was one reason given for minimalist regulation

154. Gailmard, *supra* note 148.

155. BARBARA SINCLAIR, UNORTHODOX LAWMAKING: NEW LEGISLATIVE PROCESSES IN THE U.S. CONGRESS (CQ Press 1997).

156. Cybersecurity Vulnerability Identification and Notification Act of 2020, H.R. 5680, 116th Cong. (2020).

157. *Id.*

158. BEAN, *supra* note 46.

159. *Id.*

in the 1997 U.S. Framework for Global Electronic Commerce.[160] The dynamics of information sharing, and cybersecurity generally, may move and change too quickly for an investigation that takes years—or even months to complete. For example, any investigation initiated following 2018 that reported about the lack of private-sector participation in the AIS Program likely would not reflect concerns about supply chain risks and vulnerabilities that arose on Congress's agenda the following year.[161]

C. Nominations

House committees are unable to use nominations as an oversight tool because they have no role in that process.[162] For the Senate, using the nominations process as an oversight tool presupposes the presence of nominees. As Alexander Hamilton (writing as Publius) noted in *Federalist 76*, the Senate's veto over nominations is essentially a reactive power.[163] Even if the Senate rejects a nominee, they have no guarantee the next nominee will be any more to their liking.[164] Presidents also have the option to not nominate anyone, a practice often employed in the Trump administration.[165] Because senators rely on either lower-level appointees already in office or career bureaucrats who can shift influence away from Congress, a lack of a nominee(s) would deny them the opportunity to emphasize the importance of cybersecurity information sharing and learn about future implementation plans. Issue bundling within agency jurisdictions combined with limits on attention means that even if senators did receive a nominee relevant for cybersecurity information sharing and were able to impress upon that nominee their

160. Clinton & Gore, *supra* note 90.

161. *See* Camino Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* CARNEGIE ENDOWMENT FOR INT'L PEACE (Aug. 28, 2019), https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736 [https://web.archive.org/web/20200614095441/https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736].

162. CONG. RESEARCH SERV., RL30240, CONGRESSIONAL OVERSIGHT MANUAL (2020), https://fas.org/sgp/crs/misc/RL30240.pdf [http://web.archive.org/web/20200323003037/https://fas.org/sgp/crs/misc/RL30240.pdf].

163. THE FEDERALIST NO. 76 (Alexander Hamilton).

164. *Id.*

165. John Kruzel, *Why Trump Appointments Have Lagged Behind Other Presidents,* POLITIFACT (Mar. 16, 2018), https://www.politifact.com/factchecks/2018/mar/16/donald-trump/why-trump-appointments-have-lagged-behind-other-pr/ [http://web.archive.org/web/20200323004215/https://www.politifact.com/factchecks/2018/mar/16/donald-trump/why-trump-appointments-have-lagged-behind-other-pr/].

own information sharing directives (and assuming those directives did not contradict), once in office the appointed bureaucrat still might find herself drawn into other issues and de-prioritizing information sharing.[166]

D. "Deck Stacking"

Thus far, Congress's legislative actions have served to enhance the federal government's authority to coordinate information sharing. To the extent that problems with information sharing as a policy alternative have been uncovered, Congress has focused its attention on getting agencies more access to private sector information rather than improving the quality of information that flows from agencies to companies.[167] Some enacted provisions could be interpreted as "deck stacking," such as the SECURE Act of 2018's requirement that the supply chain information sharing council engage with non-governmental stakeholders when developing information sharing standards, largely because they involve multiple agencies and, thus, different sets of interests. But here again, the changing nature of cybersecurity threats limits Congress's deck-stacking ability; legislators do not necessarily know which interests will need to be heard in the future (for example, agriculture financing interests), which means they cannot specify which interests must be represented in the administrative process without continually redefining that process and risk that some interests could be omitted.[168] The Cybersecurity Act of 2015 requires the Department of Health and Human Services (HHS) to develop a set of best practices for the health care sector, but HHS was left out of the Vulnerability Equities Process that helps decide whether to disclose vulnerabilities and threats to the private

166. Chris Bing, *New FBI Director Will Build on Comey's Cybercrime Fighting Efforts*, CYBERSCOOP (Aug. 2, 2017), https://www.cyberscoop.com/christopher-wray-fbi-cyber-crime-james-comey/ [http://web.archive.org/web/20200323004706/https://www.cyberscoop.com/christopher-wray-fbi-cyber-crime-james-comey/]; Shaun Waterman, *Cybersecurity Takes a Quiet Role in DHS Secretary's Loose Outline of Priorities*, CyberScoop (Apr. 18, 2017), https://www.cyberscoop.com/gen-john-kelly-dhs-policy-priorities-cybersecurity-musket/ [http://web.archive.org/web/20200323004834/https://www.cyberscoop.com/gen-john-kelly-dhs-policy-priorities-cybersecurity-musket/]; May et al., *supra* note 48.

167. Stephanie K. Pell, *Systematic Government Access to Private-Sector Data in the United States I,* OXFORD SCHOLARSHIP ONLINE (2017), https://www.oxfordscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-8 [http://web.archive.org/web/20200323005817/https://www.oxfordscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-8].

168. H.R. 5241, 115th Cong. (2018).

sector.[169] HHS thus could signal to health care companies that they should share information with the federal government without having a say over what information, in turn, is shared with those companies. Congress could amend the law to require that HHS be represented on the Equities Review Board but doing so might lead to lobbying from other sectors for the agencies with which they interact to also be included.

E. Casework

Casework represents another opportunity for different interests affected by cybersecurity information sharing to make their concerns known to Congress. Because casework tends to operate at the individual member level, and in the context of legislators' geographic constituency, its applicability as a cybersecurity information sharing oversight tool is somewhat limited. Cybersecurity is not a distributive policy, so legislators cannot advocate for a company in their districts and states to receive benefits.[170] To date, laws regarding information sharing emphasize that private sector participation is to be voluntary, so companies cannot really be excluded from the policy and contact their elected representative about inclusion. Members also lack clear credit-claiming incentives for encouraging companies and SLTT governments to share information when doing so might lead to negative legal or reputational consequences. And the resources and knowledge required to enable federal agencies to more effectively share information with companies and SLTT governments involve staffing and analysis, which is somewhat beyond the realm of congressional constituent service.

F. Authorization and Appropriations

The authorization and appropriations processes give Congress regular opportunities for oversight of cybersecurity information sharing,

169. Shaun Waterman, *HHS Working on Cyber Guidelines for Health Industry*, CYBERSCOOP (May 16, 2017), https://www.cyberscoop.com/hhs-working-on-cyber-guidelines-for-health-industry/ [http://web.archive.org/web/20200323010412/https://www.cyberscoop.com/hhs-working-on-cyber-guidelines-for-health-industry/]; Shaun Waterman, *Experts Ask: Why Does the VEP Cut out Health Care Agencies?*, CYBERSCOOP (Nov. 16, 2017), https://www.cyberscoop.com/vulnerabilities-equities-process-health-care-hhs-rob-joyce/ [http://web.archive.org/web/20200323010514/https://www.cyberscoop.com/vulnerabilities-equities-process-health-care-hhs-rob-joyce/].

170. John Haughey, *17 Issues Facing State Legislatures in 2019,* CONNECTIVITY (Nov. 26, 2018), https://info.cq.com/resources/17-issues-facing-state-legislators-in-2019/ [http://web.archive.org/web/20200323011207/https://info.cq.com/resources/17-issues-facing-state-legislators-in-2019/].

but some of those opportunities also are closed off by the nature of the issue.[171] Holding annual or semi-annual hearings gives committees opportunities to hear from the private sector, SLTT governments, and federal agencies about how each group thinks current information sharing policy is working. The budget process also provides Congress with quantifiable metrics of investment in policy performance, and the legislature can provide agencies with any additional resources needed. In the context of congressional oversight, however, the budget process also stands as an opportunity to sanction agencies not meeting Congress's performance standard, particularly instances of wasteful spending. In the case of cybersecurity information sharing, however, reducing an agency's budget request or authorized spending levels would work against Congress's interest by limiting agency staff levels and effectively de-prioritizing the issue.

As discussed earlier in the Article, congressional oversight is often limited without the possibility of future legislative action and other sanctions. As the preceding section illustrated, many of Congress's traditional oversight tools are lacking for cybersecurity information sharing either because of the limited utility of those sanctions or because the policy does not fit within our models of delegation and oversight in some other way. Congress finds itself placed in a position to advocate for more or better information sharing without knowing what information is not being shared that should be or, as Representative Slotkin noted, whether the information is being shared at all. In the face of limited participation in cybersecurity information sharing, Congress may find itself in a cycle of providing more and more incentives with little in the way of real sanctions (or reducing what incentives have been provided) if it is ineffective, and what sanctions it does provide may delegate further power to the other branches. The final section of this Article concludes with a discussion of whether and how we might include information sharing in our models of delegation and administrative policymaking as well as some current proposals to change how Congress conducts oversight of cybersecurity policy.[172]

---

171. BILL HENIFF JR., CONG. RESEARCH SERV., RS20371, OVERVIEW OF THE AUTHORIZATION-APPROPRIATIONS PROCESS (2012), https://www.senate.gov/CRSpubs/d2b1dc6f-4ed2-46ae-83ae-1e13b3e24150.pdf [http://web.archive.org/web/20200424213808/https://www.senate.gov/CRSpubs/d2b1dc6f-4ed2-46ae-83ae-1e13b3e24150.pdf].

172. *See infra* Part V.

V. CONCLUSION

Congress has adopted "information sharing" as a policy alternative within cybersecurity multiple times over the past decade; in lieu of broader legislative or regulatory approaches, federal agencies (particularly those in the defense, homeland security, and law enforcement domains) have been tasked with coordinating voluntary exchanges through which they can share information about cybersecurity threats, vulnerabilities, breaches, and fixes with the private sector and with SLTT governments.[173] U.S. cybersecurity policy has been marked largely by self- and co-regulation regimes, which makes cybersecurity information sharing somewhat unique as a policy alternative; the private sector, rather than federal, state, or local agencies, is expected—and expects—to play a "frontline" role.[174] Congress does not have an official role to play in these information sharing exchanges, which amplifies its information disadvantage; members do not necessarily know whether information is being shared at all, nor what kind of information is being shared. And unlike many other policies that Congress has delegated to the executive branch, agencies also face an information disadvantage: by definition, agencies do not know what information is not being shared with them.

The nature of cybersecurity information sharing as a policy alternative, thus, creates challenges for effective congressional oversight, however defined. Yet recent legislative proposals suggest a lack of concern over these challenges as Congress considers granting agencies subpoena power for certain kinds of information that would both shift additional power to the executive branch and shift the venue for debating the exercise of that power to the courts. What would it take for Congress to view agency information sharing, and particularly the expanding administrative role as new cybersecurity threats and vulnerabilities emerge, as a challenge to its own prerogatives and regulatory role?[175] Should the legislative branch even view information sharing this way? To answer these questions, we need to understand why legislators would choose to cut themselves out of the process of communication.

Our understanding of congressional oversight relies on theories of delegation: when does Congress grant more authority for developing and

---

173. ANDREW NOLAN, CONG. RESEARCH SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS (2015), https://fas.org/sgp/crs/intel/R43941.pdf [http://web.archive.org/web/20200424214303/https://fas.org/sgp/crs/intel/R43941.pdf].

174. *Understanding Cybersecurity Threats to America's Aviation Sector*, *supra* note 132.

175. Scher, *supra* note 140.

implementing policies to the executive branch, state and local governments, and other actors; how does Congress monitor the performance of those to whom authority has been delegated; and what incentives can Congress use to ensure the implemented policies align with its goals and preferences? Congress often delegates because it does not have the expertise, the time, or other resources required to regularly monitor and adjust policy. That dynamic is particularly evident for issues like cybersecurity that may change in rapid, non-linear ways as new technologies are developed and used, and new vulnerabilities and threats arise in different sectors. Understood thusly, cybersecurity information sharing as a policy alternative represents a way for Congress to economize on its attention at both the individual and institutional levels; rather than attempt to pass a new law every time technology changes and new threats and vulnerabilities emerge, Congress delegates responsibility for keeping pace with those threats to the executive branch and the private sector.

Even so, the nature of information sharing specifically within the cybersecurity domain challenges our understanding of delegation and congressional oversight in several ways. First, models of delegation typically focus on principal-agent relationships in which the public and organized interests notify Congress when the bureaucracy is not meeting its responsibilities; one of the biggest challenges currently facing cybersecurity information sharing as a policy alternative is the private sector's view that the costs of sharing information with governmental entities outweigh any benefits to doing so. To the extent that the private sector has sounded a "fire alarm" about how federal agencies are implementing the policy, it is to highlight the inadequacy of the information being shared. Second, and relatedly, many of the congressional incentives, rewards, and sanctions that are central to theories of delegation are either not applicable (as in casework or "deck-stacking" scenarios), counterproductive (such as agency budget reductions), or may be too time-intensive to keep pace with technological changes (such as investigations) for cybersecurity information sharing.

The fiscal 2019 National Defense Authorization Act established a Cybersecurity Solarium Commission, modeled after the 1953 Eisenhower Solarium Commission, comprised of members of Congress from both chambers and both parties of representatives from the Office of the Director of National Intelligence, the DHS, the DOD, and the FBI.[176] In 2020, the Commission proposed several changes to the structure of cybersecurity policymaking in both Congress and in the

176. National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (2018).

executive branch, including the addition of a select congressional committee dedicated solely to cybersecurity. Select committees must be re-authorized by Congress at the beginning of each term (unlike "standing" committees that automatically continue unless officially eliminated), and select committees typically lack the legislative authority granted to other panels.[177] While legislative authority is important for reinforcing congressional oversight as described earlier in this Article, dedicating a select committee to an issue that otherwise spans issue jurisdictions can increase attention and allow the other panels to focus on the other issues in their jurisdictions.[178] A select committee, thus, could contribute to more sustained attention to and oversight of cybersecurity information sharing.

However, the goal of having a centralized panel would still confront the reality of cybersecurity as a policy issue and the limits on policymaker attention. Cybersecurity is not only an issue itself but a component of other issues like defense, law enforcement, banking, and health care.[179] Changes in technology and cybersecurity threats and the adoption of similar technologies across economic sectors mean that the select committee's jurisdiction likely would expand over time to cover those new sectors; the prioritization problem would simply shift to a new venue. For example, cybersecurity policy has often been specifically aimed at protecting critical infrastructure, but the scope of what is considered critical infrastructure has changed over time; election systems were added in January 2017, which then expanded the institutions and actors responsible for protecting critical infrastructure cybersecurity, added election administration to any cybersecurity jurisdiction, and added a host of federal, state, and local interests to the existing competition for attention and resources within cybersecurity.

The select committee would face additional challenges depending on its status within the chamber. What incentives would members have to serve on the committee? Would it be seen merely as a steppingstone to service on a more prestigious panel? Would it attract members who are interested and engaged in cybersecurity problems or members whom leadership cannot fit in anywhere else? Would the select cybersecurity

177. A few select committees such as Intelligence and Aging in the Senate are essentially permanent, and the intelligence committees also have legislative authority. *See* CONG. RESEARCH SERV., R45421, CONGRESSIONAL OVERSIGHT OF INTELLIGENCE: BACKGROUND AND SELECTED OPTIONS FOR FURTHER REFORM, https://fas.org/sgp/crs/intel/R45421.pdf [https://web.archive.org/web/20200614110246/https://fas.org/sgp/crs/intel/R45421.pdf].

178. Lewallen, *supra* note 49.

179. Jonathan Lewallen, *Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity*, REG. & GOVERNANCE (forthcoming 2021).

committee be akin to the House Budget Committee with guaranteed seats for members of certain other committees, thereby replicating existing turf battles? What demands would members asked to sit on yet another committee make, given their already-limited time and attention? While these questions pertain to cybersecurity policy generally, the peculiarities of information sharing as a policy alternative for cybersecurity—both the nature of how it operates and the present struggles with implementation—provide Congress with only limited means to conduct effective oversight. How oversight of cybersecurity information sharing should and could function is a question both for policymakers and for our theories of oversight and delegation.