NATIONAL INSTITUTE FOR PUBLIC POLICY

INFORMATION SERIES

Issue No. 551 April 1, 2023

Cybersecurity Considerations for the New Congress

Laurin Groover
Laurin Groover spent over a decade on Capitol Hill as senior staff to House Armed Services Committee leaders. With nearly 30 years at the nexus of government, politics, and industry, she is a business development and government relations consultant specializing in cyber solutions for the warfighter.

Col. Donald J. Fielden, USAF (ret.)
Col. Donald J. Fielden recently retired from the U.S. Air Force after serving over 33 years as a cyber operations and cybersecurity leader for the Department of Defense. He currently consults for the DoD and industry on cyber operations, cybersecurity and information technology issues.

Introduction

The U.S. Government approaches to cybersecurity and protection of our national security architectures are admirably aggressive but disjointed. The disjointed approaches are yielding conflicting priorities, competing solutions, and unnecessary fiduciary expenditures. The lack of an integrated, synchronized, and strategic approach results in ever-increasing vulnerabilities to our nation's information and data ecosystem. Narrowing the aperture to Congress, there are an estimated 80 congressional committees and subcommittees that claim cybersecurity as at least part of their charters.[1] Such diversity in Congress fails to deliver a hard-hitting, enduring, and effective national-level strategic approach to securing our nation's cyber ecosystem. One solution to this problem at the national level is establishing a Joint Committee on Cybersecurity.

Given the political polarization gripping Capitol Hill, House Republicans and Democrats recently did the seemingly impossible – they came together in a bipartisan fashion to establish

the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (China Committee). The House leadership is to be applauded for addressing the serious and multitudinous threats posed by China. Both the House and Senate should expand this effort to examine more broadly the threats to U.S. cyber infrastructure critical to national security by creating a Joint Committee on Cybersecurity.

The Challenge of China

China is aggressive with its military-related cyber capabilities. The recent Department of Defense (DoD) report on *Military and Security Developments Involving the People's Republic of China 2022* details how "[t]he PRC (People's Republic of China) uses its cyberspace capabilities to not only support intelligence collection against U.S. political, economic, academic, and military targets, but also to exfiltrate sensitive information from the defense industrial base to gain military advantage and possibly for cyberattack preparations."[2] The amount and kind of information that could be extracted is staggering, as "targeted information could enable their cyberspace forces to build an operational picture of U.S. defense networks, military disposition, logistics, and related military capabilities that could be exploited prior to or during a crisis."[3] The implications cannot be understated, as "*these cyber-related campaigns threaten to erode U.S. military advantages and imperil the infrastructure and prosperity upon which those advantages rely.*"[4] (Emphasis added.)

The challenge with securing cyber infrastructure is that cyberspace knows no traditional physical boundaries. Cyberspace is defined as the "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] At its core, cyber is about data and the delivery and storage of that data. Data is critical for information dominance, and DoD has announced plans to transform itself into a data-centric organization with the goal of "improving warfighting and creating decision advantage at all echelons from the battlespace to the boardroom."[6]

Within DoD, bits of military data flow through often indescribable military and civilian pathways – and through systems owned by many entities in many countries. In fact, the "cyber" upon which military systems rely exists primarily within civilian infrastructure. Given China's extensive efforts to steal sensitive data from civilian entities in the United States, Europe, and Asia,[7] any cyber strategy designed to protect DoD systems and weapons platforms will prove insufficient unless it also addresses the civilian infrastructure upon which DoD systems rely.

The Need for a Synchronized Cyber Strategy

Recognizing the exigency of addressing cybersecurity vulnerabilities and threats posed by adversaries, DoD in 2018 took the lead in developing coordinated cybersecurity efforts with its

Cyber Strategy. The *Cyber Strategy* emphasized defending not only DoD networks but also "those networks and systems operated by non-DoD Defense Critical Infrastructure (DCI) and Defense Industrial Base" (DIB) entities.[8] It also called for "Defending Civilian Assets that Enable U.S. Military Advantage."[9]

The particular difficulty lies in the fact that the manifold, complex civilian networks that feed into the DIB and national security cyber infrastructure extend far beyond traditional military networks, and are thus outside the reach of DoD's authority. It is also important to note that DoD systems account for only part of the U.S. national security infrastructure. The additional elements of National Power – whether diplomatic, informational, and economic (in addition to military, collectively referred to as DIME) – are comprised of organizations each operating with their own unique cyber ecospheres (the people, technologies, policies, and interrelationships associated with the management and operation of cyber capabilities). And despite the 2018 *National Cyber Strategy of the United States of America,* which called for a synchronized and unified government and private sector approach to defending cyberspace, as well as the 2021 charge by Congress for the Office of the National Cyber Director (ONCD) to "[cultivate] unity of purpose and efforts across agencies and sectors" for "development and implementation of stronger national strategy, policy, and resilience for our digital ecosystem,"[10] no synchronization or unified approach across the government yet exists. A national and governmental unified approach to cybersecurity is complicated by the lack of agreement or understanding of the national security cyber infrastructure.

Congressional Action Is Necessary

While the work of the China Committee will no doubt explore the military and cyber threats posed by China, China is by no means the only competitor or adversary endeavoring to attack the cyber infrastructure critical to U.S. national security. Russia, Iran, North Korea, and numerous non-state actors are actively engaging in these kinds of attacks every moment of every day. Given that cyber is integral to every aspect of U.S. national security – every weapon system, the supply chain, power grid, and so forth – a unified national level approach is essential. And this requires greater informed congressional engagement.

Arguably, one reason for the lack of synchronization stems from uncoordinated congressional oversight, as Congress is itself stove-piped, with multiple committees overseeing various areas of jurisdiction governing cyber. For example, the House and Senate Armed Services Committees oversee the DoD and DIB cyber policy, the Homeland Security Committee oversees non-DoD agency and critical infrastructure policy, and different Appropriations Subcommittees determine how much funding is distributed for cyber initiatives across the myriad departments and agencies. And as stated previously, dozens of other committees and subcommittees have some level of cyber jurisdiction within their purview.

Congress must necessarily serve as a partner within the cyber enterprise; while the Executive Branch plans, budgets and executes, Congress is the final arbiter on government policy and funding. The congressional oversight function is critically important to ensure

Executive Branch coordination, compliance with policy, assessment of progress, and that the Executive Branch is adequately resourced for its missions.

Congress made great strides with the establishment of the Cyberspace Solarium Commission in the Fiscal Year 2019 National Defense Authorization Act (NDAA) "to develop a consensus on a strategic approach to defending the U.S. in cyberspace against cyberattacks of significant consequences."[11] Among the Commission's many recommendations was the call for establishment of congressional Committees on Cybersecurity in the House and Senate, similar to the House and Senate Intelligence Committees.

The Intelligence Committees are technically "select committees," like the House China Committee, as opposed to "standing committees." Whereas standing committees are permanent panels possessing legislative jurisdiction that includes authorization, funding, and oversight, select committees generally are created to address issues that exceed the scope of standing committees. It is important to note that because the Intelligence Committees are considered "permanent" by the House and Senate, for all intents and purposes the House and Senate Intelligence Committees are treated as standing committees in terms of oversight and authorization.

The Commission's Chairman, Senator Angus King (I-ME), pointed out regarding creation of the Intelligence Committees that "In [1976] they realized that intelligence was spread out all over the Congress and they set up committees on intelligence within the Senate and the House to consolidate that jurisdiction."[12] Cybersecurity is similarly "spread out all over Congress," highlighting the need for a unifying committee for the same reasons that led to the establishment of the Intelligence Committees.

Despite the Commission's well-founded recommendation to create House and Senate cyber committees, there are two key practical problems with establishing separate permanent standing—House and Senate select committees:

The first problem is that leaders of standing committees are loath and highly unlikely to relinquish their own jurisdiction. As Commission Chairman King noted, again with respect to establishment of the Intelligence Committees, "I don't know how they did it, because trying to do that with cyber we have found is virtually impossible . . . nobody wants to give up their little piece of the pie.''[13]

The second problem is that cyber does not fit neatly within the jurisdictional paradigm of a standing or permanent select committee. In the case of the Intelligence Committees, they oversee intelligence agencies, including elements of DoD, Homeland Security, Justice, State, Energy, and Treasury, even though standing committees have jurisdiction over these departments. The intelligence components or programs can easily be delineated jurisdictionally for oversight and funding purposes. Yet cyber is not so easily segregated as a program or activity. Again, using DoD as an example, cyber is "baked in" to weapons system programs – these programs consist of a weave of interdependent networks and data interconnected across the government and private sector. Having separate budget lines for weapons systems and their "cyber" components would be impracticable.

The most viable solution to these two problems is not establishment of a standing or permanent select committee within each chamber, but rather establishment of a "Joint" Committee on Cybersecurity to work in concert with the ONCD and provide policy and funding recommendations to the standing committees with various cyber jurisdictions. This approach would avoid jurisdictional infighting that would hinder creation of new committees, while also fostering better coordination within the government.

Joint Committees are comprised of members from both the House and Senate focused upon a particular subject area. Leadership alternates between each chamber with each new Congress. An example upon which such a joint committee should be modeled is the Joint Economic Committee (JEC). The Employment Act of 1946 established both the President's Council of Economic Advisors and the JEC. Both panels are advisory in nature, review economic conditions and suggest economic policy improvements. The JEC analyzes national economic trends and the Executive Branch response and issues policy recommendations to Congress based upon those analyses.

Similarly, a Joint Committee on Cybersecurity would be advisory in nature, review and assess coordination of current federal cybersecurity and resilience programs, analyze Executive Branch progress in addressing cyber threats, and suggest policy improvements. Committee staff would include subject matter experts who examine thoroughly the exceedingly complex and ever-evolving cyber threat landscape. Members and staff would seek input via hearings and discussions with cybersecurity leaders and experts from government, industry, and academia to further explore identified challenges and potential solutions. Synthesizing the collected information, the Committee would then develop and recommend cohesive approaches to the standing committees with cyber jurisdiction so they can implement coordinated policy and resources through appropriate legislation.

The Joint Congressional Committee on Cybersecurity would provide a holistic and 50,000-foot national focus and strategic approach that illuminates the digital ecosystems that enable the "DIME" elements of U.S. National Power, the interplay among various government (federal and state) agencies and the private sector, not just the cybersecurity and resilience requirements within a particular standing committee's jurisdiction. This would allow greater visibility into those portions of the cyber domain that tie into the national defense ecosystem.

The initial goals of this new Joint Committee on National Cybersecurity should be:

- Establish a supporting staff and panels of experts with experience and knowledge of cyber operations from across the DIME environment;
- Identify specific cyber ecosystems that are critical to maintaining U.S. power (or initial focus may be on national security) and establish policies that bring national focus to these specific ecosystems;
- Identify and prioritize vulnerabilities within each of these ecosystems. Vulnerabilities are not limited to technology and include impacts of existing laws and policies (or lack thereof), education, training, and lack of understanding of the cyber ecosystem; and,

- Working with other congressional committees and government organizations, develop recommended policies, programs, and budgets to address the most critical of priorities.

Conclusion

Such a committee is critical for providing Congress a complete picture of the cyber threat landscape so that it can effectively execute its oversight function and ensure Executive Branch synchronization that thwarts potential adversaries such as China. If the parties in power in Congress agree on nothing else, hopefully they will agree that ensuring the viability of our national security cyber infrastructure - and our decision and warfighting advantage - is an imperative.

[1] Simon Handler, "The 5 x 5 – Cybersecurity and the 117th Congress," *New Atlanticist*, October 7, 2020, available at https://www.atlanticcouncil.org/content-series/the-5x5/cybersecurity-and-the-117th-congress/.

[2] Department of Defense *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2022*, p. 70, available at https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[3] Ibid.

[4] Ibid.

[5] Catherine A. Theohary, "Defense Primer: Cyberspace Operations," Congressional Research Service, December 9, 2022, available at https://crsreports.congress.gov/product/pdf/IF/IF10537/10.

[6] Department of Defense News, "DOD Aims to Transform Itself into a Data-Centric Organization," May 10, 2021, available at https://www.defense.gov/News/News-Stories/Article/Article/2601981/dod-aims-to-transform-itself-into-a-data-centric-organization/.

[7] Sean Lyngaas, "Chinese Hackers Cast Wide Net for Trade Secrets in US, Europe and Asia, Researchers Say," *CNN*, May 4, 2022, available at https://www.cnn.com/2022/05/04/politics/china-hackers-economic-espionage-manufacturing/index.html.

[8] *Department of Defense Cyber Strategy: Summary, 2018*, available at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[9] Ibid.

[10] See Office of the National Cyber Director website at https://www.whitehouse.gov/oncd/.

[11] See Cybersecurity Solarium Commission website at https://www.solarium.gov/.

[12] Jaspreet Gill, "US Making Progress on Cyber Defense, But Up Against Some 'Significant Hurdles': Commission Report, *Breaking Defense*, September 21, 2022, available at https://breakingdefense.com/2022/09/us-making-progress-on-cyber-defense-but-up-against-significant-hurdles-commission-report/.

[13] Ibid.

INFORMATION SERIES
Issue No. 551 | April 1, 2023

The National Institute for Public Policy's *Information Series* is a periodic publication focusing on contemporary strategic issues affecting U.S. foreign and defense policy. It is a forum for promoting critical thinking on the evolving international security environment and how the dynamic geostrategic landscape affects U.S. national security. Contributors are recognized experts in the field of national security. National Institute for Public Policy would like to thank the Sarah Scaife Foundation for the generous support that made this *Information Series* possible.

 For additional information about this publication or other publications by the National Institute Press, contact: Editor, National Institute Press, 9302 Lee Highway, Suite 750 |Fairfax, VA 22031 | (703) 293- 9181 |www.nipp.org. For access to previous issues of the National Institute Press Information Series, please visit http://www.nipp.org/national-institutepress/informationseries/.