The Heritage Foundation

ISSUE BRIEF

No. 6000 | AUGUST 20, 2020

CENTER FOR NATIONAL DEFENSE

Cybersecurity: Five "Keepers" in the Cyberspace Solarium Commission Report

James Di Pane

KEY TAKEAWAYS

The current state of U.S. cybersecurity and cyber policy is not encouraging. A major cyberattack is a threat to the economy, infrastructure, and national defense.

Achieving deterrence in cyberspace must be approached holistically, with an emphasis on strengthening both offensive and defensive capabilities.

To strengthen cyber policy, Congress and the Administration should work to implement five key recommendations from the Cybersecurity Solarium Commission report.

Chartered by the 2019 National Defense Authorization Act (NDAA), the Cybersecurity Solarium Commission took a broad look at U.S. cybersecurity, the current state of cyber policy in the United States, and what policies are needed to enhance cybersecurity.

Sadly, the current state of cybersecurity and cyber policy is not an uplifting picture. The threat of a major cyberattack carries a large degree of risk for the economy, critical infrastructure, and national defense. Achieving deterrence in cyberspace should be approached holistically, with an emphasis on strengthening both offensive and defensive capabilities and an understanding that cyber interactions with adversaries are both constant and unavoidable.

The commission's report[1] itself has over 80 recommendations, but below are five of the best that should be implemented quickly to get the United States closer to solid cybersecurity ground.

This paper, in its entirety, can be found at **http://report.heritage.org/ib6000**

The Heritage Foundation | 214 Massachusetts Avenue, NE | Washington, DC 20002 | (202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

1. Appoint a Senate-Confirmed National Cyber Director to Coordinate Policy and Cybersecurity Efforts

Responsibility for cyber is currently spread throughout the government among a wide array of agencies in the Departments of Defense, Homeland Security, Treasury, and others. The role of the National Cyber Director would not be to manage these cyber functions or specific operations or policies, but rather to serve as an advisor to the President on cybersecurity and emerging tech issues and to coordinate cybersecurity operations and policies across the executive branch.

While the Director of National Intelligence as a model was raised during testimony, the commissioners suggest using the U.S. Trade Representative as a better model.[2] The position recommended by the report would reside in the Executive Office of the President, be Senate-confirmed, and be supported by a staff organized as the Office of the National Cyber Director. The appointee would be the principal advisor for cybersecurity for the President and cover emerging technology issues. The position would also lead the coordination effort for national cyber strategy, policy, and defensive cyber operations. Additionally, the appointee would also serve as the chief U.S. representative and spokesperson on cybersecurity issues.[3]

The congressional debate around the NDAA has seen efforts toward creating this position, with a Senate amendment to investigate the feasibility of the position.[4] The House version includes a provision to create the director position itself.[5]

2. Strengthen the CISA to Facilitate Cooperation with the Private Sector

The Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security is responsible for coordinating between government and the private sector to help protect critical infrastructure from cyber threats. It does this through information sharing and providing technical assistance to critical infrastructure owners and federal stakeholders.[6]

Currently, around 60 percent of CISA's budget goes toward federal programs, and only 15 percent goes to private-sector programs.[7] Expanding the CISA's budget to allow for more support of and interaction with the private sector would enhance its ability to assist in strengthening private networks. The goal should be to grow the CISA from a headquarters-type agency and develop it into an operational agency that is capable of a larger mission set and providing more operational support to both federal and private-sector partners.[8]

The sharing of threat intelligence between the private sector and government is currently a one-way street, with private organizations passing along threat intelligence to government agencies but getting very little in return due to classification. However, a great deal of threat intelligence can be safely distributed without compromising the sources and methods of collection, and the CISA should help in this effort. Further, the government should want this type of information to be widely known, as publicizing it hinders adversaries' ability to conduct attacks. The CISA would be a great organization to aggregate cyber threat intelligence to the private sector through the relationships it already has and the role it already plays.

Strengthening the CISA has also come up in the debate surrounding the NDAA and would be a strong reform to make.[9]

3. Develop a Cloud Security Certification Program

Cloud data storage—in which companies such as Amazon, Google, and Microsoft store data in the "cloud" rather than individuals or organizations hosting and securing their own data—enables more data to be stored in a more secure manner. These large companies spend millions of dollars every year to protect the data of users from cybercriminals,[10] which enhances data security. However, the fact that more data is stored together makes it a more attractive target for malevolent actors. Thus, the security of cloud services must be held to a high standard in order to ensure that user data is adequately defended.

The commission recommends developing an information and communications technology strategy for the industrial base aimed at making supply chains more secure and ensuring the availability of critical information and communications technologies. These measures would strengthen the cybersecurity of the U.S. economy and better protect intellectual property.[11] No such amendments have appeared in this year's NDAA debate.

4. Conduct a Force Structure Analysis of the Cyber Mission Forces

The Cyber Mission Forces (CMF) are the operational arm of U.S. Cyber Command. It consists of teams that conduct offensive and defensive cyber operations for the U.S. military.

The CMF was established in 2013 with a force of 133 teams of approximately 6,200 personnel. Since that time, the CMF's mission set has expanded to include election integrity and the cyber threat landscape has shifted. In congressional testimony on March 4, General Paul Nakasone, the commander of Cyber Command and director of the National Security Agency, commented that the current force has increased its operations with new authorities and that the CMF is currently too small for the tasks it is being asked to perform.[12]

Maintaining the military arm of U.S. cyber capabilities requires a force with sufficient size, training, and equipment to maintain a credible threat to adversaries. If a major part of cyber deterrence involves the ability to impose costs on adversaries, then ensuring that that capability is up to the task is vital. Congress should direct the Department of Defense to conduct a detailed force structure assessment to assess the proper size of the CMF. Also, analytic frameworks need to be developed and refined for how these forces are scaled. This proposal has also come up in this year's NDAA debate, with the Senate including it in its version of the bill.[13]

5. Strengthen Recruiting Efforts for Cyber Personnel in the Federal Government

There is a national shortage of cyber talent, making these individuals a hot commodity for federal and military service as well as the private sector.[14] This shortage is exacerbated by the fact that the number of cyber-related job vacancies continues to grow throughout the world. The federal government needs to be as competitive as possible with recruiting and retaining cyber talent, as cyber is the type of domain where talent can have an outsized effect on capability.

While the federal government will never be able to compete with the large salaries offered by the largest corporations of the world, government service has some advantages that should be exploited. Patriotic individuals will choose to serve out of a sense of duty, and certain federal programs can assist in attracting qualified candidates, such as expanded scholarship and internship opportunities and partnerships with education programs. Working for the government also allows individuals to participate in offensive cyber operations, an opportunity generally not available in the legitimate parts of the private sector. This is an aspect that can appeal to those who prefer to do more than "play defense."

Strengthening recruiting, developing, and retaining cyber talent can help the federal government attract and keep this important resource and help grow the talent pool of people interested in using their technical expertise in federal service.[15] Previous NDAAs have had measures to enhance recruitment and retention of cyber talent, and this year's NDAA continues these efforts.[16]

Recommendations

Taking the most effective advantage of the commission's best proposals will require leadership from both the Administration and Congress.

The Administration should lead the way on:

- **Conducting a force structure analysis of U.S. Cyber Command** to ensure the force is properly sized and organized to accomplish its expanded mission set and then implementing the necessary adjustments; and
- **Strengthening recruiting and retention efforts for cyber personnel** by continuing to build relationships with academic institutions, increasing outreach, and strengthening incentives to retain talent.

Congress should lead the way on:

- **Establishing a Senate-confirmed National Cyber Director** that can help advise the President and guide national cyber policy,
- **Strengthening the Cybersecurity and Infrastructure Security Agency** by increasing its budget to allow for more private-sector support and empowering it with additional authorities to share threat intelligence, and
- **Developing a cloud security certification program** by directing the National Cybersecurity Certification and Labeling Authority to work with the Office of Management and Budget and the Department of Homeland Security to develop a set of standards.

Conclusion

Cybersecurity is one of the most important issues facing the nation today, and it requires not only a whole of government, but a whole of society, response to address. These reforms and policies should get the full attention they deserve. Piecemeal reforms and stand-alone policies will not adequately address the cyber threats the nation faces.

James Di Pane is Research Associate and Program Manager for the *Index of Military Strength* in the Center for National Defense, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

Endnotes

[1] *Cybersecurity Solarium Commission Final Report*, March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view (accessed August 10, 2020).

[2] U.S. Senate Committee on Homeland Security and Governmental Affairs, "Evolving the U.S. Cybersecurity Strategy and Posture: Reviewing the Cyberspace Solarium Commission Report," U.S. Senate, May 13, 2020, https://www.hsgac.senate.gov/evolving-the-us-cybersecurity-strategy-and-posture-reviewing-the-cyberspace-solarium-commission-report (accessed August 10, 2020).

[3] *Cybersecurity Solarium Commission Final Report*, p. 37.

[4] Kelsey Atherton, "SASC Pushes Cyber Overhaul in New NDAA," *Breaking Defense*, July 1, 2020, https://breakingdefense.com/2020/07/sasc-pushes-cyber-overhaul-in-new-ndaa/ (accessed August 10, 2020).

[5] Maggie Miller, "House-Passed Defense Spending Bill Includes Provision Establishing White House Cyber Czar," *The Hill*, July 21, 2020, https://thehill.com/policy/cybersecurity/508421-house-passed-defense-spending-bill-includes-provision-establishing-white (accessed August 10, 2020).

[6] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "About CISA," https://www.cisa.gov/about-cisa (accessed August 10, 2020).

[7] *Cybersecurity Solarium Commission Final Report*, p. 39.

[8] Ibid.

[9] Mariam Baksh, "CISA Stands to Gain Powers Under Both Versions of the Defense Authorization Bill," Nextgov, July 2, 2020, https://www.nextgov.com/cybersecurity/2020/07/cisa-stands-gain-powers-under-both-versions-defense-authorization-bill/166630/ (accessed August 10, 2020).

[10] Klon Kitchen and Megan Reiss, "Ransomware Is Coming. It'll Make You Wannacry," Heritage Foundation *Commentary*, May 8, 2018, https://www.heritage.org/technology/commentary/ransomware-coming-itll-make-you-wannacry.

[11] *Cybersecurity Solarium Commission Final Report*, p. 88.

[12] General Paul Nakasone, statement before the Subcommittee on Intelligence and Emerging Threats and Capabilities, Committee on Armed Services, U.S. House of Representatives, March 4, 2020, https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf (accessed August 10, 2020). See also, Association of the United States Army, "Thought Leaders Webinar Series—General Paul Nakasone," July 20, 2020, https://www.ausa.org/events/thought-leaders-nakasone (accessed August 10, 2020).

[13] U.S. Senate, Committee on Armed Services, *National Defense Authorization Act: Fiscal Year 2021*, https://www.armed-services.senate.gov/imo/media/doc/FY%2021%20NDAA%20Summary.pdf (accessed August 10, 2020).

[14] Phil Muncaster, "Cybersecurity Skills Shortage Tops Four Million," InfoSecurity, November 7, 2019, https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops/ (accessed August 10, 2020).

[15] *Cybersecurity Solarium Commission Final Report*, p. 43.

[16] Committee on Armed Services, *National Defense Authorization Act: Fiscal Year 2021*, https://www.congress.gov/bill/116th-congress/senate-bill/4049 (accessed August 10, 2020).