Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

March 20, 2020

The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence

In August 2018, Congress authorized the Cyberspace Solarium Commission (Commission), a blue-ribbon panel tasked with examining and developing a strategic approach to defending the United States in cyberspace and protecting its advantages there. The Commission released its report on March 11, 2020. This In Focus provides an overview of the Commission and its report's findings and recommendations.

The Cyberspace Solarium Commission

Over the course of nearly a year and a half, the Commission investigated approaches to defend the nation from significant cyber attacks and ways to implement those approaches. Its authorizing legislation highlighted three policy options: deterrence, norms-based regimes, and persistent engagement with adversaries in cyberspace. The Commission was not bound to those options, and indeed expanded its research. For its work, the Commission defined priorities, conducted cost-benefit analyses, evaluated the effectiveness of the current national policy for cyberspace, and considered restructuring the federal government to manage cyber risks.

The Commission was composed of 14 commissioners—four current Members of Congress (one each from the majority and minority party in each chamber); four executive branch officers; and six non-legislative, non-executive branch members as picked by congressional leadership.

The Director of National Intelligence and the Secretary of Defense were required to provide administrative services, staff, and other support to the Commission without reimbursement. Such support included detailees from the agencies to staff the work of the Commission. Staff also included professionals from think tanks and academia. The Commission had an authorization to expend $4 million. In addition to the 14 commissioners, there were full-time staff members and part-time staff experts contributing to the work. The Commission held over 300 meetings, which included sessions with industry experts, academics, government officials, and international organizations.

The Commission borrowed its name from the Solarium Task Force—an initiative from the Eisenhower Administration which investigated strategies to combat threats from the Soviet Union. Similar to the Solarium Task Force, the Commission tasked teams to investigate different strategies and report their findings. Those strategies were then tested against opposing thoughts to advance their analysis and inform the final report.

Commission Findings and Report

The Commission found that the nation faces threats in cyberspace from nation-state actors (e.g., Russia, China, North Korea, and Iran), extremist groups, and criminals. Using cyberspace as a medium, these groups are able to exploit inherent vulnerabilities in devices, networks, and supply chains to conduct espionage, sabotage, and influence operations, according to the commission report. They also commit cybercrime (e.g., ransomware attacks) for illicit financial gain, steal intellectual property, and compromise critical infrastructure. These attacks contribute to a loss in U.S. political, military, and technological leadership, and economic advantages; and the safety of systems upon which the nation relies, the report noted.

The Commission also observed that cyberspace is a unique domain because it is relatively new, mostly owned and operated by private industry, and operates primarily by market forces—as opposed to the physical domains (i.e., land, sea, air, and space) which are more directly controlled by government.

The Commission proposed a new national strategic approach to cybersecurity: *layered cyber deterrence*. Through this approach the Commission seeks to reduce the frequency and severity of significant cyber events and limit the ability of adversaries. Layered cyber deterrence consists of four parts:

Foundation—Reform the U.S. government's organization and responsibilities.

Shape Behavior—Build a collation of partners who share our values and use our powers to influence others.

Deny Benefits—Improve national security, particularly for elections and critical infrastructure, so that adversaries are not able to use cyberspace to their advantage. Also, develop ways to ensure economic resiliency in light of cyber events.

Impose Costs—Improve cyber offensive and defensive capabilities and capacity.

The Commission's report provides recommendations for action by the Congress and the executive branch.

Selected Actions for Congress

The Commission's report groups recommendations under strategic objectives, that are organized under six policy pillars. The report contains more than 80 recommendations, of which nearly 50 would potentially need legislation. (Appendix A of the report provides an overview of all the

recommendations, and Appendix B contains a list of recommendations needing legislation).

The six pillars provide an organizing framework for the report. But as Congress considers legislation, it may be helpful to think about the recommendations with respect to changes to existing laws. Some recommendations *create* something new, others *expand* existing frameworks, and other seek to *clarify* previous laws and guidance. Those recommendations include:

- *Create Cybersecurity Committees.* This proposal borrows the concept from the select intelligence committees in the House and the Senate. Dedicated committees would have staff with requisite knowledge of cyber issues and would likely require reorganization of the current committee structure.
- *Create a National Cyber Director.* This proposal would create a Senate-confirmed position in the Executive Office of the President to oversee activities across the government for cybersecurity. The Trade Representative is a model for this proposal.
- *Create national data security and privacy protection laws.* This proposal seeks to reduce risk in the cyber ecosystem by providing certainty to companies that collect and use personal data, and any obligations they face for doing so.
- *Expand current risk management models to cybersecurity*. Many proposals fall under this category. These include improving planning for cyber-related risks, conducting national exercises, and establishing thresholds for significant events and ways the government can assist during those events, among others.
- *Expand current legal frameworks.* A few proposals are included in this category. For example, creating limits on online political advertising to address foreign influence, and expanding financial reporting requirements to include cybersecurity.
- *Expand knowledge of cyber risks.* Many proposals are included in this category. For example, improving education on digital media consumption, creating certification programs for information technology products, collecting and making available information on cyber attacks, and promoting cybersecurity insurance.
- *Codify and clarify federal agencies' roles and responsibilities.* Many proposals are included in this category. For example, the Commission recommends expanding the role of the Cybersecurity and Infrastructure Security Agency (CISA), improving the Federal Bureau of Investigation's (FBI) tools for dealing with international partners, and requiring the Department of Defense (DOD) to proactively address risks to defense industrial base (DIB) networks.

References

Included below are references on the Commission and resources policymakers may choose to examine as they consider some of the recommendations in the report.

The Cyberspace Solarium Commission

- The Cyberspace Solarium Commission website https://www.solarium.gov
- The John S. McCain National Defense Authorization Act for Fiscal Year 2019—Cyberspace Solarium Commission (P.L. 115-232, Section 1652; H.Rept. 115-874, p. 1059)

Creating Committees

- Johnson, Sullivan, Wickham, *House Practice, Chapter 11: Committees* (Washington, D.C., 2017), https://www.govinfo.gov/content/pkg/GPO-HPRACTICE-115/pdf/GPO-HPRACTICE-115-12.pdf.

CRS Reports Pertaining to Selected Recommendations

- CRS Report R44364, *The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security*
- CRS In Focus IF10654, *Challenges in Cybersecurity Education and Workforce Development*
- CRS Report R43908, *The National Institute of Standards and Technology: An Appropriations Overview*
- CRS In Focus IF10677, *The Designation of Election Systems as Critical Infrastructure*
- CRS In Focus IF10043, *Introduction to Financial Services: Insurance*
- CRS Report R45631, *Data Protection Law: An Overview*

Chris Jaikaran, Analyst in Cybersecurity Policy

IF11469

Disclaimer