Special Topic: Cybersecurity

The State of the Cybersecurity Landscape

The United States is engaged in an increasingly difficult struggle against persistent and agile cyber adversaries. U.S. companies and government agencies are spending enormous resources to secure their systems, but even the most advanced security measures are penetrable by skilled hackers.

Devices, networks and data are more connected and complex than ever before, changing the nature and scope of the cyberthreat landscape. One report estimates that the global volume of data will grow almost twentyfold from 2015 to 2025, as the Internet of Things (IoT) leads to dramatic increases in the number of connections.[1] Nearly every facet of modern life now depends on the security and resilience of cyberspace.

Cyberthreats have the potential to seriously erode U.S. economic competitiveness and undermine the benefits of innovation in new technologies. In the United States alone, The Council of Economic Advisers estimates that malicious cyberactivity cost the economy between $57 billion and $109 billion in 2016.[2] CSIS estimates that close to $600 billion, roughly 0.8 percent of global gross domestic product is lost to cybercrime each year, up from 0.6 percent in 2014.[3]

Cybersecurity as a National and Economic Security Priority

The Administration's 2018 National Cyber Strategy recognizes the importance of strengthening the country's cyber defenses and renewing the nation's commitment to a secure and competitive digital ecosystem.[4] The nation's economic and national security depends on the ability of the private sector and government to effectively defend their networks, safeguard their data, and provide secure and resilient services. U.S. private- and public-sector actors have taken important steps to boost cybersecurity investment, plan for worst-case scenarios and facilitate improved cross-stakeholder coordination, but constant vigilance is crucial against a backdrop of constantly evolving cyberthreats.

The business community is committed to building appropriate, long-standing and trusted working relationships with government partners to deploy the tools necessary to manage sophisticated cyberthreats and share cybersecurity threat information.

Looking to the Future of Cybersecurity

The U.S. approach to cybersecurity must be bolstered to address current challenges and evolving threats in cyberspace. Action should be taken to:

1. **Protect critical infrastructure.** Private-sector providers of U.S. critical infrastructure are increasingly under attack by capable state adversaries intending to exploit vulnerabilities in the event of a conflict. Government and industry should work together to identify systemic weaknesses across key critical infrastructure services, such as supply chains, and improve their collective defense through enhanced public-private partnership.

2. **Improve trust in and the resilience of digital identity**. Innovation in digital products and services requires enhanced trust and confidence in digital identity to reduce fraud. Government and industry must work together to strengthen the security and privacy of digital identity solutions by promoting the use of strong authentication technologies and moving away from solutions that are based solely on knowledge-based authentication.

3. **Promote the development, adoption and harmonization of industry best practices for securing the IoT**. Using the Department of Commerce National Institute of Standards and Technology (NIST) Cybersecurity Framework as a model, NIST should work with the private sector to develop an IoT Security Framework that incorporates industry standards and best practices. The Department of Commerce should promote harmonization of international approaches to IoT security to promote interoperability and reduce fragmentation.

4. **Ensure broad international cooperation on cybersecurity.** The federal government should support multilateral efforts that reflect the global nature of the cybersecurity challenge. This support entails harmonizing international cybersecurity measures, fostering global cybersecurity norms and promoting widespread adoption of updated international cybersecurity standards.

5. **Enhance public-private sharing of actionable cyberthreat intelligence.** Federal agencies should strengthen cybersecurity information-sharing programs by prioritizing the sharing of actionable threat intelligence between government and the private sector. Federal information-sharing programs should also be expanded to facilitate effective sharing of information related to information and communications technology supply chain risks.

6. **Prepare for future technological breakthroughs that will upend the cybersecurity landscape.** While the United States must be at the forefront of both quantum computing and artificial intelligence technologies, the country also must prepare for a future in which quantum computing can be used by other countries or bad actors to break cryptographic protocols that protect global financial markets, classified government networks, public safety and critical infrastructure networks, and other forms of communication and data that are critical to keep secure and private. Congress and the Administration should support the development of and prepare for the future deployment of quantum communications and quantum-resistant cryptography.

ENDNOTES

1 Smart, C. (2017, June). *Regulating the data that drive 21st-century economic growth: The looming transatlantic battle.* Chatham House. [Link]

2 The Council of Economic Advisers. (2018, February). *The cost of malicious cyber activity to the U.S. economy.* [Link]

3 CSIS. (2018, February). *Economic impact of cybercrime — no slowing down.* [Link]

4 The White House. (2018, September). National cyber strategy of the United States of America. [Link]