Recommendations to the President on Protecting American Cyber Interests through International Engagement

Office of the Coordinator for Cyber Issues
May 31, 2018

Prepared pursuant to Executive Order 13800, Section 3(c)

Benefits of Transformative Technology

Technological innovation has transformed the economic and social fabric of the United States and the world. Information and communications technologies (ICTs) have become a key driver of jobs, business creation, and innovation in the 21st century. They have also become an essential tool for improving the social and political inclusion of all people, including marginalized populations, across the globe. Virtually all connected communities have benefited from the adoption of these technologies, applications, and services that depend on the open architecture of the Internet. However, the growth and maturation of the use of ICTs has been accompanied by a corresponding intensification of threats to these systems and networks, as well as to the open Internet itself. These pervasive threats pose a mounting challenge to the United States which, given the global and interconnected nature of the Internet, must be addressed as both domestic and foreign policy priorities.

Challenges in an Evolving Cyberspace Environment

The United States faces innumerable threats against its networks and interests in cyberspace. Poor cybersecurity practices present a primary threat, both domestically and internationally. U.S. critical infrastructure, in particular, is increasingly interconnected and dependent on global infrastructure and systems that are vulnerable to physical and cyber threats. Countries with weak governance or rule of law can also provide safe haven for cyber criminals, terrorists, and other malicious cyber actors, or serve as hubs for exploitable machines. In addition, many countries are developing military and civilian cyber capabilities as tools for projecting influence and advancing their own domestic and foreign policy goals that may not align with U.S. interests. In recent years, malicious state and non-state actors have used cyber capabilities to: conduct cyber operations to support military and political objectives; carry out damaging and disruptive cyber attacks, including on critical infrastructure; steal sensitive and classified information from government, commercial, and civil society sources; and prepare the environment for future operations. Difficulty attributing the source of the attacks or sharing sensitive evidence to support attribution findings has made international or public-private cooperation to respond to specific threats more challenging.

The open, interoperable architecture of the Internet that enables cross-border communications, content creation, and commerce remains a key aspect of its strategic importance. As states have grasped the significance of the Internet for economic and political activity, long-standing battles to increase governmental regulation of the Internet and control speech online have intensified. Some states have come to view the open Internet and the multistakeholder approach to governing it that the United States and many like-minded countries support, as threats to their domestic stability and means to protect established Western interests. Rather than the multistakeholder approach, which is characterized by transparent, bottom-up, consensus-driven processes whereby

governments, the private sector, civil society, academia, and the technical community all participate on equal footing, these states seek intergovernmental regulation of cyberspace to diminish the role of stakeholders, and potentially fragment the Internet over issues such as censorship and flow of data. The free flow of information online, the success of U.S. law enforcement efforts, and U.S. commercial interests are at stake in this debate. There has been significant progress toward international acceptance and adoption of this inclusive multistakeholder governance model, yet challenges persist.

A New Call to Action

The President's May 11, 2017 Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" ("E.O. 13800" or "the cybersecurity E.O.") directed key departments and agencies to: (i) report on U.S. government international engagement priorities in cyberspace; (ii) develop strategies to strengthen the deterrence posture of the United States in cyberspace; and, (iii) enable the United States to engage proactively with all partners to address key issues in cyberspace.

The U.S. Department of State drafted this report to the President documenting an Engagement Strategy for International Cooperation in Cybersecurity ("International Engagement Strategy" or "Strategy") in coordination with relevant U.S. government departments and agencies, as directed by E.O. 13800. As stipulated by the cybersecurity E.O., this Strategy advances the goal of strengthening coordinated U.S. government cooperation with foreign partners and allies to address shared threats in cyberspace, thereby improving the cybersecurity of the nation. It describes the United States' priority policies, five primary objectives and corresponding actions, and three principal means of engagement to ensure continued benefits and minimized risks in cyberspace. The content herein reflects input from critical stakeholders across the U.S. government[1] and within the stakeholder community.

The U.S. Vision for Cyberspace and Approach to Cyberspace Policy

U.S. national security interests, continued U.S. economic prosperity and leadership, and the continued preeminence of liberal democratic values hinge on the security, interoperability, and resilience of cyberspace. U.S. innovation, economic growth, and competitiveness depend on global trust in the Internet and confidence in the security and stability of the networks, platforms and services that compose cyberspace. The global nature of cyberspace necessitates robust international engagement and collaboration to accomplish U.S. government goals. Accordingly, the U.S. government pursues international cooperation in cyberspace to promote its vision of an open, interoperable, reliable, and secure Internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Through international engagement, the U.S. government seeks to ensure that the Internet and other connected networks and technologies remain valuable and viable tools for future generations.

U.S. Objectives for Cyberspace Policy

[1] Contributing organizations include the Departments of State, Treasury, Defense, Commerce, Homeland Security, Justice, Energy and the Office of the U.S. Trade Representative.

Through cooperation with foreign partners and allies, and engagement with all stakeholders as appropriate, the United States will pursue the following five objectives and corresponding actions[2] to achieve its vision for cyberspace:

1. Increase international stability and reduce the risk of conflict stemming from the use of cyberspace by:
    a. Promoting international commitments regarding what constitutes acceptable and unacceptable state behavior in cyberspace from all states and how international law applies to cyberspace;
    b. Developing and implementing cyber confidence building measures (CBMs) in bilateral and regional security venues; and,
    c. Promoting a new cooperative framework in support of cyber deterrence and cost imposition on malicious state actors and state-sponsored malicious activity.

2. Identify, detect, disrupt, and deter malicious cyber actors; protect, respond to, and recover from threats posed by those actors; and enhance the resilience of the global cyber ecosystem, including critical infrastructure, by:
    a. Enhancing information sharing, including through automation and Computer Security Incident Response Team (CSIRT) channels;
    b. Managing cyber crises and responding effectively to significant cyber incidents;
    c. Improving cooperation to manage systemic cyber risk in an evolving global environment and strengthening public-private international cooperation to protect and build resilience in critical infrastructure;
    d. Promoting cybersecurity education, training, and workforce development globally to address current and future cybersecurity challenges;
    e. Prioritizing robust law enforcement cooperation;
    f. Advancing military cyber cooperation; and,
    g. Furthering cooperation on sensitive cyber intelligence issues with our partners and allies.

3. Uphold an open and interoperable Internet where human rights are protected and freely exercised and where cross-border data flows are preserved by:
    a. Defending access to an open and interoperable Internet in multilateral and international fora where it is challenged;
    b. Leveraging the existing coalition of like-minded countries that works to advance Internet freedom through diplomatic coordination; and,
    c. Supporting global Internet freedom programs that fund civil society organizations on technology development, digital safety training, policy advocacy, and applied research.

4. Maintain the essential role of non-governmental stakeholders in how cyberspace is governed by:
    a. Promoting the existing multistakeholder Internet governance system to manage key Internet resources and oppose new top-down or intergovernmental mechanisms for Internet governance; and,

[2] Objectives and corresponding actions do not necessarily appear ranked in priority order within this report.

b. Supporting the continued development, adoption, and use of interoperable, voluntary, consensus-based industry-driven technical standards.

5. Advance an international regulatory environment that supports innovation and respects the global nature of cyberspace by:
    a. Preserving a flexible, risk-management approach to cybersecurity in the global marketplace;
    b. Rejecting undue market access restrictions, including data localization requirements;
    c. Advocating for a fair and competitive global market for U.S. businesses;
    d. Encouraging private sector innovation to address security risks across the digital ecosystem; and,
    e. Maintaining a strong and balanced intellectual property protection system that includes adequate and effective enforcement of intellectual property rights, while promoting innovation.

Means of International Engagement

U.S. government engagement to achieve these objectives takes a range of forms from direct diplomatic action, to include diplomacy and foreign assistance, and joint military exercises to participation in policy and technical standard-setting bodies alongside non-governmental stakeholders. The activities outlined in this Strategy are designed to maximize the returns from U.S. government investment in international engagement towards improving the cybersecurity of the nation. Capacity building programs, in particular, demonstrate the two-fold benefit of equipping partners to assist the United States in addressing threats targeting U.S. interests in cyberspace while serving broader U.S. cyber policy, economic, and political goals. Mindful of broader national economic and security goals and foreign policy objectives, and conscious of increasing demand paired with limited resources, moving forward the U.S. government will continue to take a comprehensive, yet strategic, approach to international cooperation in cyberspace. Departments and agencies will continue to elect means of engagement that provide optimal value for both overarching and discrete needs, and that most effectively advance the U.S. vision for cyberspace, recognizing that the increasing complexity and comprehensiveness of this set of issues requires enhanced U.S. government coordination on all fronts.

Maximizing U.S. Effectiveness

This Strategy contributes to ongoing and dynamic U.S. interagency efforts to evaluate and collaborate on international engagement on cyber issues.