CYBERSECURITY

GOALS AND PRIORITIES

- Promote widespread adoption of cybersecurity best practices and frameworks, including national strategies, Computer Security Incident Response Teams (CSIRTs), public-private partnerships, and public awareness campaigns.
- Assist in cybersecurity capacity building exercises

"The United States is also working with partners to improve network defenses and in cooperation with other countries to respond to cyber incidents. All of this is crucial, because in an interconnected system like the Internet, poor cybersecurity has the potential to increase the danger for all of us. So we have to help each other. We have to maintain direct contact between our incident response teams, invest heavily in that capacity, and build that capacity so that weak spots are turned into stronger blockages against the vulnerabilities, and ultimately, they disappear."

— Secretary Kerry, An Open and Secure Internet: We Must Have Both, Korea University, Seoul, Republic of Korea, May 18 2015.

CONTEXT

The technical sophistication and range of threat actors in cyberspace has never been greater, with hacking tools, social engineering techniques, and other tradecraft in the hands of an increasing set of state actors, criminal enterprises, and 'hacktivists'. With critical systems around the world related to national security, the global economy, and social welfare now connected to the Internet, and 100 billion new devices expected to come online over the next decade, countries are increasingly concerned by realistic cyber threats that might lead to critical infrastructure failures, economic loss and financial destabilization, as well as negative impacts on the health and safety of their populations. Senior leaders in the United States now frequently cite cyber threats as the most significant security challenge facing the country, greater even than terrorism. To mitigate the risks, the United States promotes cybersecurity: the broad collection of tools, policies, best practices, and actions that can be used to protect organizations' and users' assets in cyberspace and better ensure that the intended availability, integrity, and confidentiality of online data and services are unaffected by malicious threats.

Those with poor cybersecurity pose a risk to everyone else online—a "weak link" in a global, borderless cyberspace. As such, in 2007, the United States developed a Framework for National Cybersecurity Efforts that has been a model for our national and international cybersecurity engagement. The Framework proposes five goals for nations to incorporate into their efforts toward greater cybersecurity. First: Develop national strategies to enhance cybersecurity and reduce the risks and effects of

cyber disruptions. Second: Increase government-industry collaboration (public-private partnerships) to manage cyber risk and share knowledge. Third: Fight cybercrime by updating criminal laws, procedures, and policies (see two-pager on Cybercrime for additional detail). Fourth: Develop incident management capability that can coordinate cybersecurity watch, warning, response, and recovery efforts; this capability is frequently housed in a national Computer Security Incident Response Team (CSIRT). Fifth: Build a culture of cybersecurity, increasing awareness of citizenry and industry of their critical role in protecting cyber systems (following United Nations General Assembly (UNGA) Resolutions 57/239 and 58/199). The United States is interested in coordinating more closely with partners to provide cybersecurity capacity building for those nations in need of development in any of these areas.

For many nations, the term "cybersecurity" includes efforts to combat cybercrime, to manage spam, and to protect children online. While the United States recognizes that cybercrime is in the broadest sense part of cybersecurity, we address it separately, in large part because the two areas draw on different kinds of expertise and raise different issues. The United States also distinguishes international security issues from cybersecurity, using the term "cybersecurity due diligence" to address the issues of incident response and network protection. Due diligence is very different from national security issues, including state-on-state cyber attack.

When we engage with nations on cybersecurity issues, it's important to be sure we—and they—understand precisely which aspects are being addressed. For instance, while the United States participates in the International Telecommunication Union's Development Sector (ITU-D) capacity building work in the area of cybersecurity due diligence, we do not support a preeminent role for the ITU in this area, promoting instead the value of regional approaches to the issue. The United States strongly believes that an international framework or treaty on cybersecurity would not be beneficial to the security of networks, and would divert resources from established and effective measures like national strategies and the establishment of CSIRTs. We are also concerned that some nations would use a cybersecurity treaty to reduce the free flow of information and engage in other forms of repression of online expression.

CYBER DIPLOMACY

The United States engages with many countries directly on cybersecurity through embassy contacts and senior leadership cyber consultations. In addition, the State Department has sponsored multiple cybersecurity and cybercrime capacity building workshops in Africa, with plans for East Asia as well. For more operational engagement, the U.S. government engages bilaterally through such efforts as memoranda of understanding for CSIRT information exchanges and research and development, coordinated awareness efforts, and collective action on combating botnets.

Cybersecurity is increasingly a program focus in regional organizations such as the Organization of American States (OAS), the European Union (EU), the Asia Pacific Economic Cooperation (APEC) forum, the Association of Southeast Asian Nations (ASEAN), the ASEAN Regional Forum (ARF), and the African Union (AU), and has been the subject of resolutions in the United Nations General Assembly and development efforts in the ITU-D. In addition to this set of inter-governmental fora, the United States engages with our international partners and stakeholders in operational mechanisms such as the International Watch and Warning Network (IWWN) comprised of 15 countries and the Forum of Incident Response and Security Teams (FIRST) comprised of global CSIRTs of all types (government, corporate, academic, etc.). We also engage in the Meridian Conference series and the Global Conference on Cyberspace series addressing various aspects of cybersecurity.

Office of the Coordinator For Cyber Issues (S/CCI)
United States Department of State

DESIGNED AND PRINTED BY A/GIS/GPS
AUGUST 2015