DHS Urges Global Collaboration to Boost Universal Digital Health and Security

If cyber adversaries don't discriminate between borders, the government shouldn’t, either.

Amanda Ziadeh

Fri, 03/30/2018 - 10:29

Illustration: ValeryBrozhinsky/iStock

Since its inception, the internet has been an instrument for commerce, innovation and free and open expression, but its vulnerabilities are putting all of this at risk. This cyber problem is a global one, and if adversaries aren’t discriminating between geographical borders, the government shouldn’t be, either.

“International cyberspace is growing more crowded, active and dangerous, a trend that threatens the long-term integrity of international security and order,” said Jeanette Manfra, chief cybersecurity official for the Homeland Security Department.

Manfra serves as the National Protection and Programs Directorate assistant secretary for the Office of Cybersecurity and Communications. She spoke at the Billington International Cybersecurity Summit on March 21.

As a critical component to the nation's support of allies and international partners, DHS works with federal agencies, state and local governments, and the private sector to defend against cyberthreats and protect federal civilian networks and government services.

"But our efforts cannot end there," Manfra said. Cyberthreats are not bound by national borders, and the nation's networks and the critical infrastructure they support are integrated into a global cyber ecosystem, from multinational companies to goods and services. "This really makes our usually domestic mission, inherently international," she added.

Efforts to Expand

It's time to think in terms of a global digital public health. Cybersecurity doesn't end at national borders, and neither does risk, so it's crucial to transcend them. DHS intends to do so in three critical ways.

First, it's working with partners and allies internationally to enhance operational coordination and information sharing among national computer security incident response teams. This collaboration helps protect critical networks by raising awareness of cyberthreats and sharing cybersecurity best practices.

Second, DHS supports building the international capacity to address these cyberrisks, which includes focusing on the need for collaborative efforts with the private sector to manage shared risks globally.

And third, DHS works with the departments of State, Defense and Justice to engage with counterparts abroad and reflect standard, common U.S. policies. This is part of a "whole of government" approach.

But these aren't easy tasks, and come with challenges of their own.

Assessing Risk and Global Engagement

One of most pressing obstacle is the inevitable risks associated with an increasingly global technological supply chain and connected critical infrastructure. This worldwide production of information communication technologies provides cost-effective and useful tools, but increases exposure to cyberthreats. And the movement of production outside the U.S. leads to concerns about foreign ownership, control or manipulation of items purchased by the government, or connected to the infrastructure of mission-critical systems.

And because the government depends on vendors of commercial technology, it has to do better at managing third party risks associated with a cyber supply chain.

To manage these risks, DHS collaborates with public, private and international communities and standards organizations to develop sound software development and acquisition practices. But risk assessment requires understanding system dependencies, having visibility into the supply chain process and knowing the threats.

“We work closely with the intelligence community to build a clear picture of threats we and private industry face,” Manfra added. “And we work to declassify and disseminate these insights as broadly as possible to our stakeholders.”

But rather than chasing phantom risks or the worst case scenarios, efforts should be based on hard evidence and data, and a full understanding of international threats.

“There are simply too many potentialities to account for in a diverse and active threat environment,” Manfra said.

Therein lies another challenge: establishing broader engagement, building the capacity for such risk analysis, gaining visibility of the global cyber ecosystem and partnering internationally. This may require a more thorough framework, but “overcoming these challenges is a near-term necessity,” Manfra said.

That’s largely because the threats from nation-state actors continue to escalate, and technological advancements only make that easier. Events like election interference, intellectual property theft, critical infrastructure disruption and indiscriminate targeting are growing in frequency and scale. Failing to respond to these behaviors can set a norm to cyber adversaries that they can attack with impunity, perhaps strengthening their efforts.

“We must move from a notion of traditional deterrence applied to cyberspace, to one where we are shaping the strategic threat environment," Manfra said, and modeling security toward long-term stability. But it needs to be an international initiative.

Identifying Adversaries Together

The federal government does work with domestic and international partners to publicly attribute malicious cyberactivity, and to "name and shame" those responsible. But alone, "it provides little incentive to change behavior if we are not imposing additional cost," Manfra said.

For example, on March 15, DHS and the FBI released a Joint Technical Alert providing information on a multistage intrusion campaign by Russian government cyberactors who targeted U.S. government entities and critical infrastructure sectors. This attribution included financial sanctions, which Manfra said sent a stronger message by "indemnifying this behavior and calling it out as unacceptable."

This is also where information sharing is crucial, Manfra said. By sharing this report with DHS partners and the public, she hopes it enables network defenders to identify and reduce exposure to malicious cyberactivity carried out by other nation-state actors.

Sharing Information and Standards

Outside this particular incident, information sharing is key for a secure cyber domain. It can lead to more automated defenses and a better understanding of threat behavior.

"It's a priority if we are going to secure the public health of our digital ecosystem," Manfra said.

Identifying a threat in one area could lead to building defenses against it in all areas, but only if government is fully leveraging information sharing at the scale and speed that the internet enables. For example, DHS' Automated Indicator Sharing server exchanges cyberthreat information between the government and private sector at "machine speed."

According to Manfra, more than 200 organizations are connected to AIS, including 11 international partners. Setting interoperability and common standards for threat information sharing will enable more agile and quick responses. DHS has already partnered with the international nonprofit Organization for the Advancement of Structured Information Standards, which develops open standards for the internet.

Manfra said the European Union earlier this year decided to also identify these standards for use in public procurements.

“The power of industry-coordinated and internationally-developed standards is significant, and we need to continue to leverage those,” she said.

Ultimately, it’s just too easy for attackers when nations operate independently, but it’ll take continued robust partnerships, collaboration and international engagement to protect the global online world.

“We know that we cannot secure our homeland alone. Cybersecurity is a shared responsibility. We all play a part in keeping the internet safe,” Manfra said.

View printer friendly version

Federal Cybersecurity
cyber
Department of Homeland Security
FBI
information sharing
risk
Jeanette Manfra