Data, Critical Infrastructure at Core of National Security Focus

Leaders from DOJ and ODNI discuss their strategies to protect personal data and communications integrity.

James Mersol

Mon, 07/01/2019 - 11:16

Photo credit: alexsl/istock.com

With concerns about Chinese espionage, the advent of 5G wireless networks and their effects on American national security mounting, the United States Intelligence and Law Enforcement community is at work to best capitalize on the uses of emerging technologies while also protecting against adversaries' attempts to weaponize these technologies against personal data and critical infrastructure. Leaders from the Department of Justice and the Office of the Director of National Intelligence (ODNI) spoke on the nature of these threats and what the government is doing to mitigate its risk at the DefenseOne Tech Summit June 27.

The U.S. has defended itself against both internal and external threats since its independence, but "this is different," said Principal Deputy Director of National Intelligence Sue Gordon. She identified three factors that make security in the 21st century unique: ubiquitous technology that acts as a commodity instead of a strategic advantage; global communications with low barriers to entry; and an abundance of data rather than data scarcity.

The Intelligence Community and other agencies have described cybersecurity as a whole-of-nation effort previously, but that refrain seemed especially strong Thursday.

"End-to-end [encryption] has to be part of our daily lives," said Gordon. She recognized that pushing for that level of encryption would require a culture shift around how the government processes and uses data, but that it is necessary to minimize vulnerabilities to data and critical infrastructure.

When asked how she would grade the federal government's ability to protect its infrastructure, Gordon – a self-described "really hard grader" – gave the U.S. a B "when we know it's critical infrastructure." The current challenge, she explained, is to improve the government's understanding of what counts as critical infrastructure.

The 2016 election, for example, laid bare the reality that voting systems are critical infrastructure and highlighted the need to engage state and local actors as part of the discussion. Now every sector, including energy, finance and medicine, must be involved, Gordon said.

"Despite how often we tell people about 'computer hygiene' – which really does make a difference – it's just the vastness of the threat surface is harder to protect."

Gordon encouraged everyone to remain mindful that the threat landscape is always evolving and requires a realistic, forward-thinking mindset.

“See the world for what it is,” she said. “We can’t long for a simpler time.”

Beyond engaging stakeholders at the federal, state and local levels, ODNI has recognized the importance of teaching “cyber hygiene” to everyone, not only intelligence officers, but also to eighth graders and high schoolers, said Bill Evanina, director of the National Counterintelligence and Security Center.

“If we can solve that, we can solve the supply chain problem … it starts with awareness of the threat and vulnerability,” he added.

Engaging private sector partners can be difficult, said Assistant Attorney General for National Security John Demers. In an effort to further its research into AI, machine learning and other emerging technologies, the Chinese government wants access to large data sets. Financial services, health care and other companies that hold troves of personal information are now effectively part of the national security landscape.

“That gives an intelligence officer the picture of your life,” he said. “With 99% of folks, they’ll never use [that data], but when they’re interested in somebody, they can mine into it.”

Moreover, Demers said, many of these companies want to partner with Chinese firms given the size of the Chinese market, but may not realize that the Chinese government holds a majority share in the firm, giving them the same access to any data covered under a data-sharing agreement. Demers said the government has no intention of banning companies from entering into such partnerships. His office has instead found success highlighting the firms indicted for intellectual property theft and economic espionage.

When it comes to 5G, Evanina said his office is concerned with understanding the scope of what the technology offers both as an opportunity for the U.S. and a potential threat to its security.

“We look at 5G as part-and-parcel of our whole-of-country approach to data security,” he said. “We don’t understand … our adversaries’ ability to not only target the 5G capabilities and software updates, but the ability to disrupt data, stop and rework data flows, and all of those are exacerbated a thousand times by a 5G network.”

Demers reminded everyone of the significance of the concerns behind 5G. There is no “end-state” in the 5G race or for security more broadly, he said.

“We’re learning to reap the upsides while mitigating some of these downsides,” he said. “What we’re really talking about is access to data and the integrity of our communications systems, especially in times of crisis.”

View printer friendly version
cybersecurity
critical infrastructure
5G
data protection
DOJ
ODNI
Standard