Cyber Leaders Discuss User Safety Within National Security

Major geopolitical threats target individuals at the focal point of security, experts say.

James Mersol

Mon, 10/07/2019 - 15:55

Photo Credit: erhui1979/iStock

Defense and intelligence leaders typically talk about cybersecurity as a function of state-on-state conflict or espionage. The challenge is defined in terms of hardening the United States' systems, including networks at federal agencies, critical data, research programs at top universities and cutting-edge technology in the private sector, against attacks from foreign espionage.

Even thinking about the threat at that macro level, it is important to think about both the threat and the solutions to it at the micro level, recommended cybersecurity experts speaking at the Washington Post Live Cybersecurity Summit last week. The threat vectors commonly target the user, and by protecting American citizens, the U.S. can continue innovating while defending against espionage, stalkers and other malicious actors online.

When asked about how the National Counterintelligence and Security Center (NCSC) frames the national security challenge from China — in terms of IP theft, economic espionage, technology race, spy agency versus spy agency, or spy agency versus private sector — Director William Evanina answered, “all of the above.” The center thinks about those vectors both individually and as parts of a whole, he said, adding that the Chinese Ministry of State Security has representatives throughout its government and in several private firms, giving it a reach unlike any counterpart in the U.S.

The 2014 indictment of Chinese agents who stole intellectual property from American firms was “a watershed moment” for working with the private sector, Evanina said. Even though the U.S. and China do not have an extradition treaty, it highlighted the risks the private sector must consider, even if their technology is for a benign purpose.

“In the case recently with utilization of Duke and Yale’s capability for genome mapping — sometimes we engage with [China] and do great collaborative work … and they take it anyway,” Evanina outlined. “They took that technology on genomes and DNA, and they used it to imprison over a million Uighurs. Even great technology that we utilize for great purposes is sometimes used nefariously by intelligence services of rogue nations.”

Other speakers at the event focused on cybersecurity for the individual, focusing on a personal safety perspective in addition to the threat identity theft and spyware can pose to an organization or agency.

“Most people who are being spied on … are not being spied on by governments or law enforcement,” explained Eva Galperin, director of cybersecurity for the Electronic Frontier Foundation. “They are being spied on by stalkers, or by exes, or by people with whom they are currently in an abusive relationship.”

The threat models have not adapted to this trend because they assume that having access to a username, password and approved devices is enough to verify someone’s identity, Galperin added.

“Abuse often involves access to all of these things at once,” she said. “Now we need to completely rethink our threat models.” Some cybersecurity firms are already working on how to “take all of these threats seriously,” recognizing the risk to personal safety as well as the organizational and criminal aspect.

“We’ve seen nation-state actors using the same kind of spyware that abusive partners wind up using,” said John Scott-Railton, a senior researcher for Citizen Lab, a research institute at the University of Toronto. “It just works because human behavior is … unpatchable.”

Both the public and private sector should consider the solution to this problem, given the ramifications, he added.

In sum, the speakers throughout the morning were optimistic, but encouraged vigilance for new threats and threat vectors going forward. Panelists speaking on personal cybersecurity generally agreed that circumstances will improve for users worried about identity theft and what they described as “stalkerware." Attackers are already having to work harder to circumvent today’s security, they said and platforms overall are more secure than ever.

On the other hand, they said, the threat surface is growing “exponentially” thanks to the number of smart devices entering the market, and security approaches to the "internet of things" are still in their nascent stages.

At the macro level, protecting American research is a crucial focus for security.

“We are still the cradle of innovation,” said David Hickton, a former U.S. attorney for the Western District of Pennsylvania, who now serves as the founder and director of the University of Pittsburgh’s Institute for Cyber Law, Policy and Security. Following the 2014 indictments, in 2015 his office uncovered a ring of fraudulent SAT and GRE test-takers who were helping to forge credentials for Chinese spies to attend America’s researchers. Both he and Evanina mentioned that it is important to welcome the best and brightest from across the world to the U.S., while keeping out those — from any nation — whose sole goal is espionage.

“Recently, the FBI and Department of Justice charged and indicted an American citizen on a university campus for spying for the Chinese intelligence service," said Evanina. “It’s not about Chinese individuals and students who are here. It’s about the Communist Party of China and how they manifest their efforts here in the U.S. through the Ministry of State Security.”

View printer friendly version
China
cyber
Federal Cybersecurity
safety
internet of things
malware
Standard