DHS Secretary: US Will Fight Back Against Foreign Cyber Enemies

But what exactly those measures mean is unclear.

Camille Tuutti

Wed, 04/18/2018 - 12:14

DHS Secretary Kirstjen Nielsen spoke at the RSA Conference in San Francisco.
Photo: Camille Tuutti/GovernmentCIO Media

SAN FRANCISCO — Any digital adversary looking to strike against the U.S., a word of warning: just don't. The federal government is done playing nice and will not only chase down hackers and nation-state enemies but will punish them accordingly, said the secretary of homeland security.

Speaking Tuesday at the RSA Conference in San Francisco, DHS Secretary Kirstjen Nielsen delivered a keynote with strongly worded caution for those who attempt to target the nation. And there are plenty who try.

“The cyberthreat landscape is different today,” she said. “Cyber is not only a target; cyber can be used as a weapon and has the attack vector for other nefarious activity.”

For example, “infrastructure can be hijacked and held hostage,” she said, something we saw with the worldwide WannaCry ransomware attack in May 2017. And institutions can be compromised to undermine the democratic process — as seen with Russia’s meddling in the 2016 U.S. presidential election.

Last year was especially bad in terms of the number of high-profile, widespread cyberattacks.

Nearly half of all Americans’ sensitive information was compromised when credit bureau Equifax suffered a massive data breach. Then, the WannaCry ransomware ravaged the world, paralyzing millions of Windows computers and demanding victims pay a ransom to unlock their data. Petya and NotPetya, two other ransomware variants, also froze untold computers in various sectors, causing disruption throughout the world.

The NotPetya attack was “one of the costliest cyber incidents in modern history,” Nielsen said.

“By 2021, cyberthreat data alone is expected to hit $6 trillion annually,” she said. “To put that in perspective, that’s almost 10 percent of the world economy.”

Making matters worse, the expansive ecosystem of internet-connected devices makes it easier for cyber adversaries to attack because of the myriad entry points. And cybercrooks are increasingly “bolder, more brazen and savvier than ever before,” she added.

That's especially true of nation-state attackers.

Perpetrators’ methods have changed from sloppy and predictable to “sophisticated and sinister,” Nielsen said. The federal responses to these evolving attacks are complicated by attackers’ different objectives, so there’s no “one size fits all

approach," she added.

While some foreign governments want to siphon U.S. classified information and pilfer intellectual property, sensitive personal information or trade secrets, others "simply want to understand our patterns and behaviors and choices to manipulate us," Nielsen said.

These adversaries are "often indifferent to collateral damage," she said. But these high-profile attacks mean high risk, something most cybercrooks tend to avoid. So why do they keep happening?

"The answer is simple: They think they can get away with it, and too often they have," Nielsen said.

But no more.

After Russia's interference with the U.S. elections, it's time to put the kibosh on bad behavior that influence U.S. matters, Nielsen said. Today's threats "are so severe that if we don't start identifying and punishing our assailants, they will overtake us," she said. In her role, Nielsen said she is working with her counterparts in the president's cabinet to fight back.

"Complacency is being replaced by consequences," as Nielsen put it.

"The United States possess a suite of response options, both seen and unseen, and we will use them to call out bad behavior, punish it and deter future cyberhostility," she said. "So, those who try to attack our democracy, to affect our elections . . . or to undermine our national sovereignty, I have a simple word of warning: don't."

When asked about what type of consequences would be appropriate for cyberattackers, Nielsen hinted at more proactive defense rather than taking actual offensive measures, including strong partnerships and policy efforts.

"We need to get to a point where we agree on terms," Nielsen continued, and violating those should mean real consequences. But as for hacking back, DHS isn't quite there, though the topic does come up in conversations, Nielsen said.

"There are many things we can do around . . . proactive defense, for example, to prepare our systems, to prevent intrusion of nefarious activity or traffic," she said.

View printer friendly version

cybersecurity
DHS
natsec
Kirstjen Nielsen
Russia
WannaCry
RSA Conference
election