Homeland Security Outlines Plan to Protect US Elections

With midterms quickly approaching, DHS launches coalitions, task forces and governmentwide initiatives to thwart another Russian election meddling.

Amanda Ziadeh

Thu, 07/12/2018 - 11:46

Photo Credit: Homeland Security Committee

In 2016, the Homeland Security Department issued a statement with the U.S. intelligence community about the Russian government's intention to interfere with the U.S. election process, compromising emails from citizens, institutions and political organizations. Current threats to election security, however, are information-based, and DHS is working to identify them before the midterm elections.

"Our mission at DHS is to help our stakeholders better understand and manage the

risks they face through concerted efforts, in part by building relationships, establishing trust, and understanding what it is that our stakeholders need to manage their risks," said Christopher Krebs, undersecretary for DHS' National Protection and Programs Directorate. He testified at the Homeland Security Committee's hearing on securing elections systems and critical infrastructure on July 11.

Krebs said NPPD has made significant progress by working with local and state election officials and the private sector partners who support them, creating cross-sector councils, sharing information and developing strategies to reduce risk to the nation's election systems.

NPPD created the Election Infrastructure Information Sharing and Analysis Center, or the EI-ISAC. Since its inception in February, the center has nearly 1,000 members, comprised of all 50 states and local jurisdictions.

But what does the current election security threat landscape look like for the 2018 midterms in November, and how are DHS' efforts helping to mitigate them?

Technical Attacks vs. Information Operations

Along with email hacking, DHS' statement included states reporting the scanning and probing of their election-related systems. But so far, according to Krebs, DHS has not seen anything to the degree of the 2016 election interferences, in terms of the specific hacking of election systems.

So, it's important to differentiate between the types of threats in this space. Directed technical attacks against IT systems, like Russia's attempts into the voter registration database and scanning of those systems in 2016, is the cybersecurity technical piece of it, Krebs said to the committee.

Then there's information operations. And while DHS isn't seeing the directed and focused election campaign medalling like it did in 2016, "the intelligence community continues to see Russian activity in the sowing discord across the American public," Kreb said.

It’s not necessarily directed at politicians or political campaigns, but on identifying divisive issues, encouraging controversy and disagreement, creating chaos and undermining democracy.

So in terms of campaign information warfare, Krebs said DHS is currently seeing information operations rather than directed technical attacks or anything specifically focused on the midterm elections.

Threats to IT Election Systems

In terms of vulnerabilities in voting systems, from electronic poll books to the backend information management systems that store voter registration, Krebs said there are vulnerabilities by nature. And Russian adversaries’ ability to scan these IT systems is an automated process. They scan looking for vulnerabilities and infiltration points, and that’s the threat, Krebs said.

There are a series of compensating controls that can limit risk of IT systems, however, “and ultimately, what we’re looking for here is not 100 percent secure system,” Krebs said. “Just like any IT system, there is no such thing as a secure IT system. What we’re looking for is resilience in the system,” where if something happens, the system can keep moving forward.

In other words, IT systems have technical challenges. But even if the database of an election system is compromised and a registered voter is intentionally deleted from a voter registration file, the citizen has the ability to request a provisional ballot upon arrival, vote, and have that vote count. So, even if Russian adversaries had accessed registration databases and deleted voter registration files, Krebs said it wouldn’t have impacted a citizen’s ability to vote.

And knowing state election systems have been scanned is all about visibility into the system traffic and networks, which Krebs said DHS has much more of going into the 2018 midterm elections than it did in 2016.

Since February, NPPD has quadrupled its insights into state election system activities with the help of all 50 states participating in the EI-ISAC, and with the deployment of intrusion detection system sensors to those election systems, Krebs said. By November, NPPD will have access to, and nearly 100 percent visibility into,

all the state networks, and other jurisdictions.

Awareness and Action

Identifying, responding to and protecting the nation from these kinds of cyber activities is a governmentwide effort. Krebs said DHS has duties in both the technical hacking side, as well as information operations.

“DHS has lead for supporting state and local governments in the hacking space. FBI has lead in the countering foreign interference and information operations space. DHS does support the FBI’s efforts, as does, of course, the Intelligence Community,” he said.

To that point, in order to make the information and products DHS pushes out immediately actionable by a broad community, Krebs said he aims to operate as much as possible in the unclassified space. The information DHS provides is intended to be useful, especially to those at the state and local level.

“It doesn’t help me if I’m living in a classified space, that should not be the DHS mission space. We should be managing risk in an unclassified manner that’s informed by threat intelligence,” Krebs said.

Cross-Industry Collaboration

As noted, FBI leads information operations, but DHS does support. So the FBI’s role working with the Intelligence Community is identifying specific actors, whether that be twitter handles or other form of social identity, and disrupting those activities.

But taking down the disruptive activity is only part of the problem. “The way to counter this information is to actually shine light on the activity,” Krebs said.

So, NPPD works with the State Department’s Global Engagement Center and the FBI to build a greater understanding and awareness of what these adversarial actions are. Then, they engage with social media companies and traditional media to share findings and trends, to identify the types of things adversaries are doing and how to raise awareness to the American people.

“It’s different from traditional cybersecurity,” Krebs said. Election systems need to be resilient, but “disinformation is completely different, the objective is

antifragility.” So, rather than just moving through a hit, the goal is to come back stronger, learning from that experience or engagement.

NPPD is learning from Russia’s 2016 election meddling and working to close that avenue of influence. NPPD is doing trend analysis of how Russian actors engage through information campaigns and operations, and looking for open opportunities of intervention to close.

This is an inter-agency and cross-government effort, too. The NPPD works with DHS’ intelligence and analysis office, privacy office, civil rights and civil liberties office, and has established a Countering Foreign Intelligence Task Force. This task force works in coordination with the FBI’s Foreign Influence Task Force (which deals with election interference), and is supported by the Intelligence Community.

“Everybody has a role in this, given the unique authorities of the various agencies,” Krebs said.

But the DHS task force isn’t meant to be an incident response capability. It’s more of an analytical cell to track activities, tactics, techniques and procedures over time to build a body of knowledge to share, Krebs said, while agencies like FBI have the more tactical response.

Once that information and analysis is identified, it’s a government-industry collaboration to notify the public and take action. Social media companies work with government to be able to identify misinformation or propaganda-based accounts, flag it or take it down.

“This is truly a partnership,” Krebs said. “The government will be taking certain actions, and then the private sector will be taking certain actions.” Just look at recent reports of Twitter suspending more than 70 million accounts in May and June alone, for example. “That’s the sort of activity you’ll see going forward,” Krebs said.

Other efforts by NPPD to convene federal government and election officials regularly to share cybersecurity risk information, and to identify areas where DHS can help, include the Election Infrastructure Subsector (EIS) Government Coordinating Council. The GCC holds weekly meetings and includes DHS, the Election Assistance Commission, and 24 state and local election officials, according to Krebs’ testimony.

“We need to work with our stakeholders to understand what their requirements are so that we can tailor our services to address their needs,” Krebs said.

Beyond Information Sharing

So, what has NPPD learned from watching recent Russian adversarial activity, like its cyber attacks on Ukraine’s power grids, and the U.S. Computer Emergency Readiness Team’s joint statement on Russia government’s cyber activities targeting the U.S. energy and critical infrastructure?

“They’re getting better,” Krebs said. “Each subsequent incident shows that increase level of capability.”

NPPD is looking at the capability that they demonstrate, what the corresponding vulnerabilities are, the exposure and risk level in terms of U.S. systems and networks, and how DHS can work with the critical infrastructure community to help them understand and respond to that risk.

And critical to this is moving beyond information sharing. “Information sharing is the foundation of how you manage risk,” Krebs said, “what we need to do, to continue to move into, is a risk management integration space.”

This means avoiding the siloes of these systems, because whether it’s industrial control systems or general IT systems, they’re almost agnostic to sectors or they cut across several sectors, Krebs sai.,

“So we need to be working cross-sector, government-industry together, to do integrated risk assessment, integrated strategic planning and integrated risk mitigation strategies,” Krebs said. That’s something NPPD is focused on right now; taking threat intelligence and working with industry to decide what that threat intelligence means and what to do about that knowledge.

Because adversaries are getting better at these strategic attacks — as opposed to opportunistic attacks, like ransomware — particularly in the hard infrastructure and operational IT space of energy, critical manufacturing, transportation, and aviation, Krebs said.

In response, NPPD is kicking off the National Risk Management Initiative to focus on moving beyond intelligence and into risk management, understanding what the

problem is and how to properly address it. “I think that’s where we’re going to make the most significant gain,” Krebs said.

View printer friendly version
cyberattacks
election
Russia
Federal Cybersecurity
Department of Homeland Security
FBI
Intelligence Community