America, Democracy and Cyber Risk: Time to Act

Prepared Statement
by
Honorable Eric Rosenbach
Co-Director of the Belfer Center for Science and International Affairs at Harvard Kennedy School; former Chief of Staff to the Secretary of Defense and Assistant Secretary of Defense for Homeland Defense and Global Security

Before the

United States Senate Committee on Homeland Security and Governmental Affairs

Hearing on

Mitigating America's Cybersecurity Risk

April 24, 2018

Chairman Johnson, Ranking Member McCaskill, and distinguished members, thank you for calling today's hearing on mitigating America's cybersecurity risk and for the invitation to testify.

This is a time for action, and your Committee should play a key role. If American leaders in both the private sector and government continue to admire and debate our cyber vulnerabilities, the things that define the United States will steadily erode: democracy, a vibrant free-market economy, and the very values and freedoms that have guided our country since its foundation.

Here are some of the threats we've seen just this month: sophisticated ransomware shut down the city government of Atlanta for more than a week. Ransomware previously deployed by North Korean cyber operatives hit aircraft production lines at a major Boeing facility. DHS revealed that Russian cyber operatives have compromised major aspects of the internet's routing infrastructure. A recent White House report by the Council of Economic Advisers predicted that the cost of cybercrime to the US economy is set to top $100 billion annually.

The most concerning cyberattacks haven't yet cost the nation a dime, but could result in catastrophic consequences: DHS recently confirmed that Russian military intelligence operatives emplaced the malware used to take down the Ukrainian power grid (twice!) throughout energy infrastructure in the United States. And, as we approach the 2018 midterm elections, the risk of Russian cyber and information attacks against our election systems and campaigns is very real.

Against this backdrop, it is crucial that the nation comes together to build real capability and take real action to address these threats.

Russia is not the only potential threat. North Korea, Iran and China also maintain sophisticated offensive cyber capabilities. These countries also enjoy asymmetric advantages over the United States in cyberspace. Authoritarian societies often control their domestic media, censor online activity, and shield their citizens from outside information and cyber operations through national firewalls, such as the Great Firewall of China. Over the weekend, China's President Xi signaled that his government will increase its already tight control over internet and social media content as a national security priority, and Russia also has been intensifying its crackdown on internet and media freedoms in the past two years.

By contrast, the United States is a digital democracy. Our technological advances, high levels of digital connectivity, and transparent, open society make us vulnerable to foreign cyber and information attacks. In short, we live in a digital "glass house."

The cyber threat landscape we face is congested, and complex. Our adversaries are increasingly willing to attack non-government networks and private citizens, and to engage in widespread, indiscriminate attacks. North Korea's "WannaCry" cyberattack in 2017 affected organizations worldwide, including temporarily derailing operations at the UK's National Health Service. Russia's 2017 "NotPetya" cyberattack initially targeted Ukrainian organizations, but spread across the world, caused operations at major global transport and logistics companies to grind to a halt, and costing the private sector billions of dollars in damages.

As we look to the rest of 2018, the signals are clear: even organizations that are not targets of cyber attacks will be victims. From a CEO's perspective, the threat of collateral cyber damage is sobering—planning for and managing cyber risk has never been more complicated.

From the government's perspective, our adversaries' willingness to attack civilian targets makes the attack surface that we need to defend incredibly large. How should we prioritize resources and strategize for defense when the potential attack surface extends from government networks in D.C., to home routers in Wisconsin, hospital networks in Missouri and logistics hubs in Ohio, and everything in between?

This hearing and the Committee's framing of the problem we face—as one of *managing* cyber risk—are important. We will not eliminate cyber threats to America. To manage this cyber risk, the US Government must help lead a whole-of-nation effort to:

1. Bolster our domestic capabilities for defense and resilience;
2. Develop precise and legal offensive cyber capabilities to disrupt cyber and information attacks at their source; and
3. Adopt a clear, public deterrence posture.

Bolster domestic defenses and resilience

Cyber risk affects all corners of our economy and society. It is a whole-of-nation threat. It can only be successfully addressed with a whole-of-nation effort. The Government has a leading role to play. But ultimately, actions by private enterprise and non-government organizations will be key to our success.

Congress can do more to incentivize the private sector to act. In particular, Congress should:

- mandate that critical infrastructure providers adopt the NIST Cybersecurity Framework;
- establish baseline security standards for the manufacturers and distributors of "internet of things" devices, such as home routers, thermostats and security systems; and
- ensure that online platforms—including Facebook, Twitter, and YouTube—are not used as tools for foreign adversary information operations.

Bolstering private sector cyber defenses without regulation should be a priority. For example, one important lever to improve cyber risk management is a properly functioning market for cyber risk insurance. The government, and DHS and FBI in particular, can play a role in helping to unlock the promise of a mature cyber insurance market by improving collection and access to anonymized cyber incident data.

Significantly, DHS must empower the private sector to bolster its cyber defenses by continuing to strengthen information sharing with high-risk sectors. This is particularly urgent for election cybersecurity.

Organizations outside government must also play a role in protecting the nation from cyberattack. The Defending Digital Democracy Project, a bipartisan initiative I co-lead at Harvard's Belfer Center—along with Robby Mook and Matt Rhoades—works very closely with states to improve their ability to mitigate cyber risk. It's clear that the states take the cybersecurity of their systems very seriously. But states simply are not equipped to face the pointy-end of the spear of cyber attacks from state adversaries who are spending billions of dollars and dedicating thousands of cyber operators to advance their national interests.

Over the past nine months, our team of hard-working students, cyber security experts, technologists and political operatives:

- conducted field research at 34 state and local election offices;
- observed the November 2017 elections in three states;
- conducted a nationwide survey on cybersecurity with 37 states and territories; and
- engaged state and local election officials in three national "tabletop" simulations.

Our research and work found that under the leadership of Secretary Nielsen, Under Secretary Krebs and Assistant Secretary Manfra, DHS has improved information sharing with the states. We also saw that the Department's efforts to provide real capability are important: cybersecurity scans and risk assessments to the states have been productive and help mitigate risk. Congress should strongly support these efforts and provide DHS with the resources it needs to bring them to full maturity.

DHS has shown that bringing real capability to the table is essential. Congress should support the development of DHS' cybersecurity capability by providing the resources and authority for the Department to establish a robust, operationally-focused cybersecurity agency. This is more than bureaucratic box-shuffling: the nation needs an organization that provides critical infrastructure operators with the type of expert-level support that could make a real difference in mitigating the risk of foreign cyberattack.

And when it comes to protecting elections and critical infrastructure, state governments should look closely at strengthening the role that the National Guard and state-run fusion centers play in election-related threat information sharing. This potent combination will provide an important hub for sharing threat intelligence and cybersecurity capability.

Develop precise and legal offensive cyber capabilities

Even with improved cyber defenses, we will of course not be immune from attack. To complement the work that DHS does, the US Government, led by the Department of Defense, must bolster real capabilities to disrupt and degrade cyber and information operations at their source. In particular, there is a need to:

- **Strengthen indications and warning of cyber and information attacks.** The Intelligence Community, and the National Security Agency in particular, need to bolster the "early warning" system for information operations which target US democratic institutions.
- **Bolster Cyber Command's capability to address information operations.** The US military lacks the structure and capability necessary to defend the nation from future attacks. Special Operations Command has historically led Department of Defense efforts in information operations, but the lead must now shift to Cyber Command in order to strengthen the nexus of cyber and information operations capabilities necessary for the information age. That said, the Department of Defense's recent efforts to combat ISIS through a joint SOCOM-CYBERCOM effort, known as Task Force Ares, represents an outstanding model for future operations.
- **Take a leading role in building international capacity to disrupt the proliferation of black-market destructive malware.** The Proliferation Security Initiative for weapons of mass destruction—supported by over 100 countries—provides an analogous model for action.
- **Take a more active role in disrupting and dismantling botnets used by criminals and foreign adversaries.** Law enforcement organizations, led by the FBI and Department of Justice, alongside the Department of Defense when needed, should work very closely with telecommunications companies and international partners to neutralize botnets.

Adopt a clear, public deterrence posture

Our national response to cyber and information attacks—both against the United States and our allies—has been consistently weak.

Imagine if we found out during the Cold War that Soviet operatives had placed secret explosives in parts of the electric grid all around the United States. Would US leaders have stood by and debated the nature of the threat, or would they have acted?

The United States must urgently act to bolster its cyber deterrence posture by both raising the costs of attacks and decreasing the benefits to hostile actors of engaging in cyber and information operations. Recently, the increased willingness of the Intelligence Community, DHS and FBI to publicly attribute attacks to foreign is crucial and a positive first step. This must happen more

often, and more swiftly, and be accompanied by consequences. The recent move by the current administration to increase sanctions on Russian entities involved in cyber attacks against Ukraine and the United States is another step in the right direction, but again not nearly enough.

We also need to more consistently respond to cyberattacks against our allies and partners. Russia frequently uses Ukraine and other of its neighbors as "testing grounds" for its offensive information and cyber operations. However, Las Vegas rules do not apply in the digital age. If we permit Russia to test and perfect these tools on another country, they will eventually be used against us. Additionally, as the NotPetya cyberattack I spoke about earlier demonstrates, even attacks that are intended to only affect entities in one country can enter the global supply chain and quickly spread to damage US actors and interests.

In sum, defending our nation from state adversaries is ultimately a government responsibility. But we will never be able to deter or defend ourselves against all cyberattacks. The United States became the world's technological leader by harnessing the talents of thousands of public and private sector innovators. To protect our technological edge, and our nation, we must once again mobilize all parts of society in a whole-of-nation effort.