"Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks"

Prepared Statement
by
Honorable Eric Rosenbach
Co-Director of Belfer Center at Harvard Kennedy School; former Assistant Secretary of Defense for Homeland Defense and Global Security

Before the
United States Senate Foreign Relations Committee
Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy

Hearing on

State-Sponsored Cyberspace Threats: Recent Incidents and U.S. Policy Response
June 12, 2017

Chairman Gardner, Ranking Member Markey and other distinguished members of the Committee, thank you for calling today's hearing on cybersecurity and for the invitation to testify.

As technology advances and we become more connected, we increasingly live in a digital "glass house" that must be much better protected. I like to use the glass house analogy because it helps illustrate two important points.

First, that cyber warfare is truly asymmetric: a small nation with an offensive cyber capability can have an outsized effect on a larger power. For example, the US—a technological and economic powerhouse—is significantly more vulnerable to cyberattack than North Korea, a nation where most citizens do not even have an internet connection. We should therefore think very carefully about the implications of a possible North Korean cyberattack on the United States, something that I believe is likely to happen within the next year if current trends continue.

Second, that democracies' transparent, open societies also make them vulnerable to foreign information operations. This vulnerability is exacerbated by high levels of internet accessibility and the rapid pace and breadth of information sharing. In contrast, authoritarian societies like China, Russia and North Korea often control the media, censor domestic online activity and shield their nations (to some degree) from outside information and cyber operations through the use of national-level firewalls, such as the Great Firewall of China.

Unfortunately, no nation, including the United States, has responded to Russia's recent potent hybrid of cyber and information attacks in a way that is visible and forceful enough to deter future attacks. The fragility of our national cybersecurity posture, combined with our adversaries' perception that Russia's recent actions achieved unprecedented success, increases the likelihood that the US and our allies will experience more serious attacks in the coming years.

Thus, the US needs to bolster its deterrence posture by both raising the costs and decreasing the benefits to hostile actors of engaging in this conduct.

In 2015, the Department of Defense articulated for the first time our strategy on deterrence in cyberspace. In sum, the strategy articulated that deterrence is partially a function of perception. As the DoD strategy explains, deterrence works by "convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed."[1]

In terms of increasing the costs of an attack, the US and international community should be less circumspect about employing all available foreign policy tools, particularly those outside of the cyber domain. Given the "glass house effect" that I previously described, we should be careful about responding to cyberattacks with military options since the US has more to lose from an escalation in cyber-initiated conflict. We should, however, be prepared to use our superior cyber capability strategically and creatively in order demonstrate our willingness to act in the face of serious provocations.

Additionally, the US must increase the costs of cyber and information operations by using foreign policy tools outside the military domain, such as: 1) attributing publicly cyber and information attacks as soon as we have confidence the origins; 2) pushing for sustained multi-lateral economic sanctions against states that use cyber and information weapons; 3) reinventing our capabilities with respect to information operations and our strategy for countering them; and 4) taking a leading role in building international capacity to disrupt the proliferation of black-market destructive malware.[2]

As I mentioned, reducing the benefits that adversaries derive from cyber and information operations is a key aspect of bolstering our deterrence posture. To do this, the Administration, Congress and private sector should work together to: 1) pass legislation that improves the ability

[1] The Department of Defense Cyber Strategy, April 2015, p.11.

[2] By disrupting the black market for destructive malware and other exploits, the international community would increase the costs associated with conducting? cyber and information attacks. This is a difficult challenge, but the Proliferation Security Initiative for weapons of mass destruction—a global initiative supported by over 100 countries—provides an analogous model for action.

for the government and private sector to share cyber threat information, including with state election bodies and campaigns; 2) legislate mandatory compliance with the NIST's Cybersecurity Framework for critical infrastructure providers; 3) pursue more aggressive steps to mitigate the effect of information operations on the platforms of leading tech companies, including Facebook, Twitter and Google; and 4) incentivize investment in cloud-based security, blockchain-enabled transactions and quantum computing.

Developing and employing operational cyber capabilities is an important way to advance US national interests. That said, we simply must keep sensitive vulnerabilities and exploits secure. Allowing this type of sensitive knowledge to get into the public domain damages American tech firms and increases the likelihood that hostile actors will conduct malicious actions against the US.

In sum, the strength of the tech sector and the internet has driven American economic growth and strengthened our democracy for the past two decades. The corollary of this success, though, is that the US is increasingly vulnerable to cyber and information attacks. In order to maintain the "center of gravity" for the United States, we must bolster America's cybersecurity posture and rethink our strategy for countering foreign information operations.