Testimony

Emerging Cyber Threats and Implications

Isaac R. Porche III

RAND Office of External Affairs

CT-453

February 2016

Testimony presented before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on February 25, 2016

For more information on this publication, visit www.rand.org/pubs/testimonies/CT453.html

Published by the RAND Corporation, Santa Monica, Calif.

Isaac R. Porche III[1]
The RAND Corporation

Emerging Cyber Threats and Implications[2]

Before the Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
U.S. House of Representatives

February 25, 2016

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee, thank you for inviting me to address important emerging concerns related to cyberspace and cybersecurity. Specifically, I will discuss how cyberspace continues to change, expand, and remain inherently vulnerable. I will discuss both the kind of information sharing that is needed to help defend cyberspace proactively and how the public's privacy concerns affect that very information sharing. Finally, I will mention the needed next steps, including more discussion of the need to balance security and privacy, potential technological approaches, and the potential need for future legislation.

Introduction

Since the creation of the ARPANet—the Internet's predecessor—kaleidoscopic change has been the single constant of the information environment. What started out as a relatively wonky communications tool for a smallish group of engineers, scientists, and computer experts is now a global information infrastructure: "a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location."[3]

Today, it is useful to think of the information environment as two partially intersecting areas: social networks and cyberspace (Figure 1). Social networks are the webs of interactions and relationships among individuals. They are continuing to grow in size, relevance, and influence, affecting not only how we communicate with one another but if and how we find employment,

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT453.html.

[3] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "Brief History of the Internet," InternetSociety.org, undated.

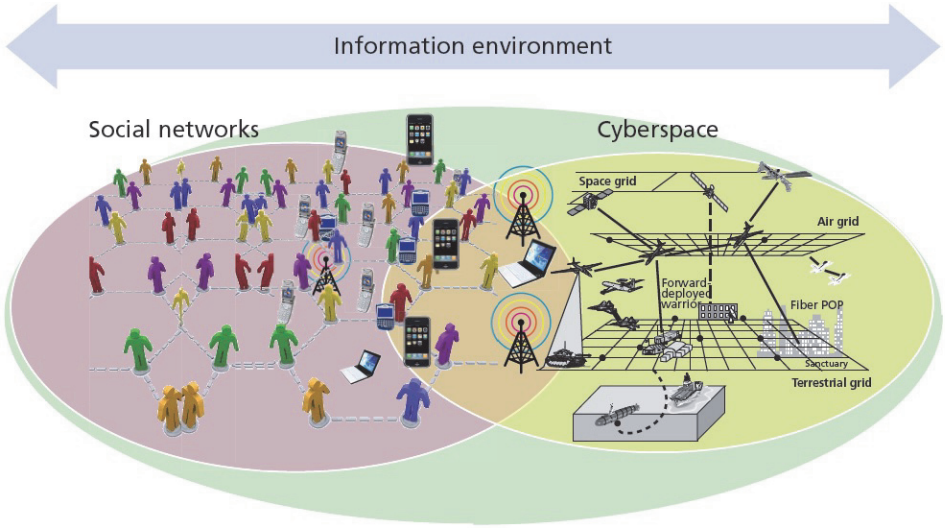
housing, and romantic relationships; but social networks are also influencing the evolution of modern conflict. The so-called Islamic State, for example, has successfully used the social-networking platform Twitter to persuade distant potential recruits to literally—physically—mobilize.

Cyberspace is the technical foundation on which the world relies to interact, exchange information, conduct business, and so on. It is, according to the Joint Chiefs of Staff, a

> global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[4]

Cyberspace is both a global domain and a global commons whose reach is being constantly expanded not only by wired and wireless connections, but by sneaker-netted connectors that close all air gaps.[5] Everything from home thermostats to the critical infrastructure that is vital to daily life—water, power, manufacturing, etc.—is within its reach. It is "shared by all" and currently dominated by none. Eventually, controlling cyberspace (and the intersecting electromagnetic spectrum) could be tantamount to controlling the information environment.

Figure 1. The Information Environment Includes Social Networks and Cyberspace



SOURCE: Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy M. Daehner, and Bruce J. Held, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, Santa Monica, Calif.: RAND Corporation, MG-1113-A, 2013.

[4] Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12R, February 5, 2013.

[5] *Sneakernet* is an informal term that describes using physical media (e.g., thumb drives, CDs) rather than a computer network to move electronic information from one computer to another.

The rapid pace of change makes it difficult for even nimble corporations to keep up with emerging threats and to close newly discovered vulnerabilities, and the challenge for the U.S. government is even greater. Governmental controls and processes make rapidly acquiring materiel difficult, and it is also difficult to make rapid changes in personnel structure. Thus, keeping up with major changes, such as the merging of the wired and wireless worlds, poses formidable challenges to all.[6]

Two Trends in Cyberspace

For a moment, think of cyberspace as a balloon that's constantly being filled with more and more air. As the balloon gets bigger, the amount of surface area that is vulnerable to a pinprick increases, the skin of the balloon stretches and gets thinner, and the volume of air trapped inside grows. I use the balloon metaphor to help illustrate three key points about today's cybersecurity environment:

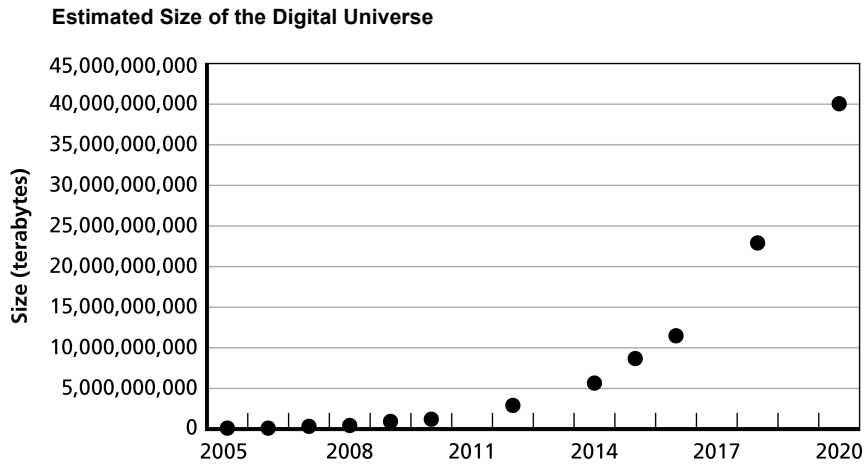
- First, like the surface of the balloon, **the "attack surface area" of cyberspace is expanding every day as more and more devices are brought online.** Some estimate that, right now, there are billions of Internet-connected devices—a number that could surpass a trillion in just ten years.[7] Each smartphone, computer, tablet, television, refrigerator, and "intelligent" vehicle is a potential cyber target.
- Second, like the skin of the balloon, **cybersecurity resources—which are already stretched thin—must try to keep pace with increasing complexity as new devices come to market and become interconnected.** For example, if you upgrade your old home security system to a new one that connects to your smartphone, you have complicated the task of protecting your home by introducing several cyber vulnerabilities.
- Third, like the air inside the balloon, **the amount and type of data we are all actively and passively uploading to the Internet is constantly expanding.** One popular traffic app for smartphones constantly monitors your location, even when you are not using the app. You have to actively turn this feature off if you do not want your phone to share your

[6] Most of the language and analysis in this section is drawn from Porche et al., 2013.

[7] Estimates vary. In 2014, Gartner, Inc., forecasted that 6.4 billion Internet-connected devices would be in use worldwide in 2016, and that 20.8 billion would be in use by 2020. "In 2016," Gartner predicted, "5.5 million new things will get connected every day" ("Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015," Gartner.com, press release, November 11, 2014). In 2015, *Business Insider* estimated that 10 billion devices were connected worldwide and that 34 billion will be connected by 2020 (Jonathan Camhi, "BI Intelligence Projects 34 Billion Devices Will Be Connected by 2020," BusinessInsider.com, November 6, 2015). In 2015, Juniper Research suggested that the number of Internet-connected devices will reach 38.5 billion in 2020 ("'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020," JuniperResearch.com, press release, July 28, 2015). According to the 2016 Georgia Tech *Emerging Cyber Threats Report*, there could be a trillion devices by 2025 (Institute for Information Security and Privacy, *Emerging Cyber Threats Report 2016*, Georgia Institute of Technology, 2015).

location with the app—and with the app's partners—every single minute. The entire "digital universe" is already billions of terabytes and constantly growing. Estimates of the annual growth of this universe vary, but the increases appear to be exponential (see Figure 2).[8]

Figure 2. The Digital Universe Is Growing Exponentially



SOURCE: Porche et al., 2014.

So, cyberspace is expanding, becoming increasingly vulnerable, and hosting increasingly vast amounts of (sometimes critical) data. That's the first trend. The second trend is that **the number of bad actors seeking to exploit cyberspace for criminal or malicious purposes is growing too:** "Since the mid-2000s," RAND Corporation experts warn, "the hacking community has been steadily growing and maturing."[9] In 2014, more than a billion personal data records were compromised by cyberattacks—a 78 percent "surge" in the number of personal data records compromised compared with 2013.[10]

Considerable numbers of people and organizations—including highly organized groups with cartel, terrorist, or even nation-state connections[11]—are constantly trying to prick the balloon, and pins are a dime a dozen. Tools for bad actors in cyberspace are, quite literally, commodities:

---

[8] The estimates and projections in the section are drawn from Isaac R. Porche III, Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, and Evan Saltzman, *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information*, Santa Monica, Calif.: RAND Corporation, RR-315-NAVY, 2014.

[9] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Santa Monica, Calif.: RAND Corporation, RR-610-JNI, 2014.

[10] Arjun Kharpal, "Year of the Hack? A Billion Records Compromised in 2014," CNBC.com, February 12, 2015.

[11] Ablon, Libicki, and Golay, 2014.

They can be—and are being—bought and sold. For example, cyber criminals have sold login credentials for Facebook in bulk,[12] even as more and more sites are encouraging users to log in using their Facebook accounts. Training in malicious hacking can be acquired easily and for free online on sites you probably visit a few times a week, like YouTube. Experts agree that the coming years will bring more activity in so-called darknets, and more use of crypto-currencies; that the ability to stage cyberattacks will continue to outpace the ability to defend against them[13]; and that there will be more hacking for hire.[14] Furthermore, a body of research is emerging called automatic exploit generation (AEG) that seeks algorithms that automatically generate large quantities of exploitable bugs.[15]

Why These Trends in Cyberspace Will Persist

A number of factors guarantee that cyberspace will continue to expand, continue to become increasingly vulnerable, and continue to host increasingly vast amounts of (sometimes critical) data:

- the shift to digitized information (e.g., voice, video, and data)
- the miniaturization of computing and data-storage devices that carry digitized information, coupled with low costs, which has fostered an explosion of increasingly networked digital devices
- continued growth in wired and wireless networks and electronic systems, which make it possible to access, via the Internet, systems that used to be isolated (i.e., offline)
- the accelerating deployment of digital control systems that operate physical systems, from cars to aircraft, from home thermostats to the power grid, and so on

---

[12] Amit Klein, "Fraudsters Selling Login Credentials for Facebook, Twitter in Bulk," SecurityIntelligence.com, February 8, 2012.

[13] This is a viewpoint echoed by former Deputy Secretary of Defense William Lynn in *Foreign Affairs*:

> In cyberspace, the offense has the upper hand. . . . [T]he U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks' weaknesses. . . . In an offense-dominant environment, a fortress mentality will not work. (William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010.)

[14] Ablon, Libicki, and Golay, 2014.

[15] According to Matthew Ruffell's overview of AEG (Matthew Ruffell, "Applying Bytecode Level Automatic Exploit Generation to Embedded Systems," Christchurch, New Zealand: University of Canterbury, October 16, 2015), Brumley et al. discovered in 2008 that it was possible to automatically generate an exploit by analyzing a vulnerable binary program and the patched binary program by comparing the two and pinpointing what code had been changed and ultimately output an exploit. See David Brumley, Pongsin Poosankam, Dawn Song, and Jiang Zheng, "Automatic Patch-Based Exploit Generation Is Possible: Techniques and Implications," *IEEE Symposium on Security and Privacy, 2008*, May 18–22, 2008, pp. 143–157.

- the increasing popularity of online media and social networking, which, according to one study, has led some people to spend more time each day on a phone or laptop (an average of 8 hours and 41 minutes) than sleeping[16]
- the combined decrease in cost, increase in speed, and standardization of interoperating electronic systems, which not only make these systems more accessible to anyone but also increase the potential for exploitation.

These and other trends enable any government or state to use capabilities that were once available only to developed countries with large defense budgets, although it should be noted that these capabilities simultaneously increase the exposure of those countries. Additionally, individuals who were previously considered noncombatants can now join the battle and wage silent, electronic war. Finally, as information systems become ubiquitous, our reliance on them increases apace. Today's modern economic, political, and military systems depend more than ever on information and instructions generated in cyberspace nodes and transmitted across a vast network. Such reliance invites conflict and exploitation.

Options to Address the Emerging Landscape in Cyberspace and Obstacles to Implementing Them

So, who do we have working on building a tougher skin for the balloon, taking pins off the market, and tracking down and stopping would-be pin-prickers? We have good guys: cybersecurity professionals, "white hat" hackers, and other individuals who are identifying and patching vulnerabilities and who are trying to take down the bad actors. However, at the moment, in the U.S. government, there simply are not enough of these good guys to go around.[17] Educating, recruiting, training, and hiring cybersecurity professionals takes time, and the most-capable professionals—the elite commercial "cyber ninjas"—can command salaries that the government simply cannot match.[18]

Aside from hiring more good guys, what are our options for improving cybersecurity? One of the best options is improving information-sharing and cooperation between and among government entities and the private sector. The Cybersecurity Information Sharing Act of 2015, which contains elements to help facilitate information sharing, is one effort that could stimulate the kind of

---

[16] Madlen Davies, "Average Person Now Spends More Time on Their Phone and Laptop than Sleeping, Study Claims," DailyMail.co.uk, March 11, 2015.

[17] Joe Davidson, "Lack of Digital Talent Adds to Cybersecurity Problems," *Washington Post*, July 19, 2015.

[18] Martin C. Libicki, David Senty, and Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market*, Santa Monica, Calif.: RAND Corporation, RR-430, 2014.

information sharing that is needed.[19] Why is sharing of discovered vulnerabilities, defense measures, and best practices so important? Because bad actors benefit from slow identification and slow mitigation of a threat.[20] Given the time taken to identify a malicious intrusion and determine its extent, which is usually measured in months, the bad actors are long gone, along with your data.[21] If government entities and the private sector were sharing information quickly and often, they have a better chance of being able to anticipate and prepare for an eventual attack. So, beyond just identifying and responding to attacks more quickly, threats have to be anticipated and the behavior of threat actors known. Intelligence on threat actors and their intentions is a necessary ingredient to significantly improve the chances of predicting and identifying the next act.

Unfortunately, several factors make this kind of information sharing and cooperation a lot easier to talk about than to actually implement. First is the fact that cyberspace is largely a private-sector construct, subject to private-sector concerns. Working against the pursuit of perfect (or even good-enough) security is the need to get software and hardware to the market quickly, at a competitive price, and with all the innovative features none of us yet know that we absolutely cannot live without. As of June 2015, developers were submitting more than 1,000 apps to Apple every day for evaluation.[22] At that kind of volume, Apple cannot be expected to validate that every single app it approves is perfectly secure—no matter how it is used, no matter what other apps the user runs, and whether those apps are updated as needed. The result is a sprawling universe of software and hardware, some of which is, as the 2016 national threat assessment put it, "designed and fielded with minimal security requirements and testing . . . [such that they] could lead to widespread vulnerabilities in civilian infrastructure and [U.S. government] systems."[23]

The second obstacle to this kind of information sharing and cooperation is that most of the U.S. public is simply not comfortable with the idea of mass government surveillance. Specific attitudes toward this issue are nuanced and complex, but the Pew Research Center reported that, in 2015,

---

[19] This includes sharing of knowledge about cybersecurity threats (including vulnerabilities), indicators of cybersecurity threats (e.g., malicious reconnaissance), and sharing of defensive measures and best practices.

[20] Many attacks come after the announcement of a vulnerability and release of a patch: "When software vendors announce and ship patches, hackers analyze the patches and can often develop exploits for the problem faster than companies can install the patch" (James A. Lewis, *Raising the Bar for Cybersecurity*, Washington, D.C.: Center for Strategic and International Studies, February 12, 2013).

[21] According Mandiant's 2015 threat report, *A View from the Front Lines*, the median duration that threat groups were present on a victim's network before detection was 205 days.

[22] Jerin Matthew, "Apple App Store Growing by Over 1,000 Apps per Day," IBITimes.co.uk, June 6, 2015.

[23] James R. Clapper, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," presented to the Senate Armed Services Committee, February 9, 2016.

65 percent of U.S. adults believed that "there are not adequate limits on the telephone and internet data that the government collects."[24] Frankly, even the most well-meaning proposals to increase information sharing between the government and the private sector can feel like something out of George Orwell's *1984*.

However, despite private-sector imperatives and public concerns about a "Big Brother" nation, there are real, serious threats to, from, and in cyberspace: threats to American citizens, American businesses, and critical national infrastructure. It will be increasingly difficult for the U.S. government, along with state and local agencies—including law enforcement—to pursue and prosecute cyber criminals and other nefarious actors without some kind of continued information sharing and cooperation that has occurred routinely in the past. The likely court fight emerging now between the Federal Bureau of Investigation and Apple over unlocking the phone of one of the San Bernardino attackers is a timely example. It is worrisome to privacy advocates that are concerned that this is a "test case for the general principle that [the government] should be able to compel tech companies to assist in police investigations."[25]

Bureaucratic and Legal Issues That Can Hamper Defense

Defending against sophisticated attacks against critical infrastructure (such as Stuxnet, a computer "worm" allegedly designed to sabotage Iran's nuclear program) requires excellent capabilities marshaled into a coherent and coordinated response. The United States has plenty of the former but, in my view, has difficulty conducting the latter. Responsibilities can overlap or conflict. For example, stealing financial information is a crime, and the Federal Bureau of Investigation is charged with dealing with such criminal activity. However, the Department of Homeland Security has a mandate to protect the civilian agencies of the federal executive branch and to lead the protection of critical cyberspace.[26]

Good intelligence has always been a prerequisite to good defense, but many attacks come from overseas locations. Therefore, efforts to garner intelligence outside the United States would involve the agencies authorized to do so. Many regard the National Security Agency as the most capable government entity when it comes to analyzing and defending against cyber attacks. But legal limits constrain what the U.S. Department of Defense and Intelligence Community can do.

---

[24] Mary Madden and Lee Rainie, "Americans' Attitudes About Privacy, Security and Surveillance," PewInternet.org, May 20, 2015.

[25] Ben Adida, "On Apple and the FBI," Benlog.com blog post, February 18, 2016.

[26] Further, the Defense Department has responsibility for defending U.S. national interests against cyberattacks of "significant consequence."

Much illicit activity masks itself in emails, but privacy laws preclude how much the government can monitor such transmissions.

None of this is to say that these carefully defined limitations cannot be overcome. Indeed, a number of proposed pieces of legislation attempt to deal with them. However, the challenge is great and is compounded by the speed needed to respond to increasingly sophisticated threats. Worms can be scrubbed from systems if its administrators know the systems have been breached. But they need to act within the window of opportunity, whether that is days, weeks, or months. Otherwise, the worm will have done its damage and then erased itself.[27]

The Way Ahead

To better prepare to mitigate the emerging threats and improve the cybersecurity of this country, two overarching goals should be pursued continuously:

- First, **enable substantially better information sharing and collaboration among key departments and agencies** (Department of Justice, Department of Homeland Security, Department of Defense, and Office of the Director of National Intelligence) **and the private sector.** The Cybersecurity Information Sharing Act of 2015 was a needed, but small and careful, step toward this goal, in part because it encourages the private sector (via liability protections) and U.S. government to share knowledge of cybersecurity threats, including classified vulnerabilities, best practices, and defensive measures. This law could better enable the community to anticipate attacks and have a more proactive defense posture.
- Second, **achieve unity of effort across the U.S. government.** Today, different government agencies have different cyber responsibilities. This makes perfect sense in many ways, because different agencies have different capabilities, so they should be tasked to do what they are good at doing. The trick is to harness all the capabilities to a common end, and therein lies the problem. Cyber defense requires a coherent response, and the bureaucratic responsibilities as currently articulated hinder progress toward that goal. President Obama's appointment of a Chief Information Security Officer for the

[27]The language and analysis in this section is drawn from Isaac R. Porche, Jerry M. Sollinger and Shawn McKay, *A Cyberworm that Knows No Boundaries*, Santa Monica, Calif.: RAND Corporation, OP-342-OSD, 2011.

country—part of his newly announced Cybersecurity National Action Plan[28]—is another careful small step toward some needs.[29]

Ultimately, perhaps ideally, what is needed is **the ability to track cyber intruders, criminals, and other hostile actors in cyberspace with the same freedom of maneuver (and speed) these adversaries enjoy.** Achieving this goal will require a sustained, long-term effort. New authorities will be required, along with substantial revisions to the U.S. Code (a daunting challenge). Public debate will be lively. Indeed, I have long argued that public debate is a critical first step:

> Government intrusion into private affairs, even for reasons of the common defense, evokes an emotional response. . . . A first step requires an honest, public debate [that] calls into question the very firewalls between public and private sectors that are intrinsic to democracy.[30]

Furthermore, what is needed is a discussion of how to best balance the need for security and privacy. There are many ways to facilitate this kind of discussion, and the proposal put forth by Full Committee Chairman Michael McCaul and Senator Mark Warner is one way to move forward, though there could be others.

It is fair say that today's debate about whether device makers should be required to build "backdoors" into operating systems so law enforcement and intelligence agencies can collect data has jumpstarted this much-needed discussion. This is a good thing.

In the short term, the next steps are multipronged. Congress needs to continue to develop strong, smart policies and laws designed to improve cybersecurity—laws like the Cybersecurity Information Sharing Act of 2015. Although there is an immediate need for such policies and laws, Congress would be well advised to incrementally design these policies and laws, and communicate them to the public, to earn the public's confidence in the government's ability and intentions. Specifically, the public must be convinced that the government's information needs are balanced with individuals' desire for privacy. At present, many ideas for, and approaches to, using

---

[28] The White House, Office of the Press Secretary, "Fact Sheet: Cybersecurity National Action Plan," February 9, 2016. A related news article noted that "the Obama administration is creating a new high-level federal official to coordinate cybersecurity across civilian agencies and to work with military and intelligence counterparts, as part of its 2017 budget proposal announced Tuesday" (Tami Abdollah, "Obama Administration Plans New High-Level Cyber Official," ABCNews.com, February 9, 2016).

[29] For example, government information technology modernization.

[30] Isaac Porche, "Stuxnet Is the World's Problem," *Bulletin of the Atomic Scientists*, December 19, 2010.

technology to improve cybersecurity—such as pooling and mining vast stores of data—alarm those who believe in a right to privacy from government intrusion.[31]

There also needs to be appreciation that everyone has a role to play in improving cybersecurity:

- The **U.S. government** should continue to facilitate and encourage information sharing and cooperation between and among government entities and the private sector to protect citizens, businesses, and critical infrastructure against cyberthreats. Department of Homeland Security Secretary Jeh Johnson has just recently announced preliminary guidance for information sharing between the private sector and the U.S. government.[32] Eventually, the U.S. government should also find ways to exploit all forms of data and intelligence to identify and anticipate both threats and bad actors, without unacceptably infringing on individuals' desire for privacy.
- **Developers and purveyors** of Internet-connected software and hardware—including large corporations, individual app developers, and everyone in between—need to be equipped to understand the security impacts of their work.[33] Today, a software developer does not need to have a degree, or any formal training, or any license whatsoever to write programs that control our infrastructure. There are few, if any, engineering fields that find themselves in a similar predicament. For example, the design of a drawbridge requires the oversight and approval of a licensed civil engineer, whereas anyone, in theory, can design the software that controls that bridge. Cybersecurity is everyone's responsibility, from the chief information security officer to the individual app developer.[34]
- **Individual consumers** should do more to protect their software, hardware, and private information. Simply put, most of us are either too busy or insufficiently educated (likely both) to spend our days and nights patching every device in the home. We often keep old and impossible-to-secure devices and computers up and running. As the President's Cybersecurity National Action Plan notes, there is too much old, outdated equipment online today, which makes for easily targeted entry points and "botnet soldiers."[35]

---

[31] For example, big data analytics in support of cybersecurity.

[32] Aaron Boyd, "DHS Releases Initial Guidelines for Cyber Threat Info-Sharing," FederalTimes.com, February 17, 2016.

[33] Threats and vulnerabilities can originate anywhere, including the usual suspects (e.g., known hackers) or even well-intentioned amateur code writers. A malicious hacker with a laptop and a seat in an Internet café has everything needed to launch an attack in cyberspace. Alternatively, a well-intentioned but naïve "app writer" can accidentally propagate a useful utility that unlocks backdoor access.

[34] Many technology companies insist that they have to train all new employees, whether hired with a degree or not, on techniques for secure development. There is a gap in our educational system at all levels.

[35] The White House, Office of the Press Secretary, 2016.

There is no simple solution to the threat posed by adversaries in cyberspace. However, one critical challenge that must be overcome—soon—is determining how to protect the cybersecurity of a democratic society that demands both freedom and privacy in its use of computer systems and networks from the threat posed by enemies who respect no boundaries and can act largely with impunity, despite national and international norms and legal frameworks.

Thank you for your time and I am happy to answer any questions.