U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

February 27, 2015

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on "Understanding the Cyber Threat and Implications for the 21st Century Economy"

I. INTRODUCTION

On Tuesday March 3, 2015, at 2:00 p.m. in 2322 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled "Understanding the Cyber Threat and Implications for the 21st Century Economy." This will be the first in a series of hearings focused on cyberspace, the Internet, and the challenges and opportunities that they present. Cyberspace has become the backbone and engine of the 21st century economy, and recent high-profile information security breaches have raised awareness of the vulnerabilities and risks facing cyberspace. With this hearing series, the Subcommittee seeks to expand the discussion surrounding these issues to examine the broader implications for businesses and consumers in today's 21st century economy. This initial hearing will provide an overview of the issue, focusing on the history, evolution, and future of cybersecurity.

II. WITNESSES

- Herbert Lin, Senior Research Scholar at the Center for International Security and Cooperation and Senior Fellow at the Hoover Institution, Stanford University;

- Richard Bejtlich, Chief Security Strategist, FireEye, Incorporated; and,

- Gregory Shannon, Chief Scientist, CERT Program, the Software Engineering Institute, Carnegie Mellon University.

III. SUMMARY

Over the past two-and-a-half decades, society has become increasingly dependent on the Internet. Governments use it to interact with their citizens. Businesses use it to develop global markets. Individuals use it to connect with each other. Without question, the Internet and resulting explosion in information technology have introduced incredible convenience, prosperity, and freedom of expression to nations across the globe.

At the same time, this new technology introduced the world to a new challenge – cybersecurity. Every day, the public is flooded with reports of new breaches, vulnerabilities, or potential risks stemming from weaknesses in the digital infrastructure that drives the 21st century economy. With every new incident, whether it is the theft of consumer data, a nation-state sponsored attack on a corporation, or an intrusion into our nation's critical infrastructure, there is renewed discussion about the need for cybersecurity "solutions." There is relatively little discussion, however, about what this means for businesses and society. For example, how will improved information security affect the pace of innovation? To what extent are consumers willing to sacrifice convenience in the interest of security? How can costly security solutions keep pace with threats that constantly evolve?

Cyber threats are rooted in the fundamental structure of the internet. The same technological and cultural factors that facilitate the strengths of the Internet (e.g., real-time global interaction, rapid innovation, and freedom of expression) enable malicious actors to thrive and create risk in cyberspace. There is no way to "solve" the cybersecurity problem without compromising the benefits of a connected, digital world. Therefore, efforts to minimize the cybersecurity threat require careful consideration of the social, economic, and cultural costs of improved security.

IV. BACKGROUND

A. History and Evolution of the Internet

In the late 1960's, the Advanced Research Projects Agency (ARPA)[1] funded an innovative project called ARPANET. The project sought to realize a concept first described by Massachusetts Institute of Technology researcher, J.C.R. Licklider in 1962 – an interconnected network of computers that could remotely share data and information.[2] In late 1969, four computers located at the University of California at Los Angeles, Stanford University in Palo Alto, the University of California at Santa Barbara, and the University of Utah connected to the ARPANET, proving Dr. Licklider's networking concept and laying the foundation of what is now known as the Internet.[3,4]

What began as a handful of closed networks used by a small and trusted number of parties has evolved into a vast network of networks. These networks range in scale from point-to-point links such as smartphones to massive "backbone" networks that collect, carry, and share information from numerous small networks over vast distances.[5] All of these individual networks

[1] The Advanced Research Projects Agency has since changed their name to the Defense Advanced Research Projects Agency (DARPA). *See* www.darpa.mil.

[2] Internet Society, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (last visited Feb. 26, 2015).

[3] *Id.*

[4] The term Internet was formally agreed upon in 1995 by the Federal Networking Council.

[5] COMMITTEE ON DEVELOPING A CYBERSECURITY PRIMER: LEVERAGING TWO DECADES OF NATIONAL ACADEMIES WORK, NATIONAL ACADEMY OF SCIENCES, AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY: SOME BASIC

are able to interact seamlessly because the Internet was designed be an open platform, based on common architecture and protocols, to transmit data from one location to another. The devices, services, and applications attached to the network remain responsible for processing the data.[6] In other words, the Internet acts simply as a conduit for information.

This open architecture concept is the fundamental basis of the Internet's success. Because the Internet simply transports data and does not discriminate against the applications and devices connected to the network, it creates endless possibilities for innovation. This open framework enabled and continues to foster the development of programs such as email, smartphone applications, and cloud computing. It has introduced previously unimaginable efficiencies for businesses and opened new markets across the globe. It has given individuals a voice and revolutionized the way in which societies learn and consume information. As a result, the Internet has grown to be not just a technological curiosity, but an integral element of modern society.

All of these benefits rely on information technology, comprised of the computing and communications devices and protocols that connect to the Internet.[7] The Internet has therefore driven the massive development and integration of these technologies in our daily lives. Today, we depend on information technology for everything from personal communication to energy distribution. This integration of the Internet and information technologies into nearly every aspect of modern life has created the virtual world commonly known as *cyberspace*.[8] While not easily defined, cyberspace encompasses all networks and information technology, their information and interconnections, both on and off the Internet.[9] While the growth of the Internet and cyberspace provide tremendous benefits to society, they also introduce a new challenge – cybersecurity.

B. Cybersecurity: Threats and Challenges

Complex Systems Create Vulnerabilities

To a standard user of the Internet, the act of visiting a web page is a series of straightforward steps. That user knows to open a browser, enter the web address of the site that he or she wish to view, and then wait for the requested web page to appear. Rarely does one realize, however, the many steps and technological innovations that allow that "straightforward" process to occur. Figure 1 depicts a flowchart of the steps that the information technologies involved in a website request must take in order to successfully display a web page.

CONCEPTS AND ISSUES 21 (David Clark et al. eds., 2014), *available at* http://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic [hereinafter *Primer*].

[6] Internet Society, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (last visited Feb. 26, 2015)

[7] *Primer, supra* note 5, at 8

[8] Lance Strate, *The varieties of cyberspace: Problems in definition and delimitation*, 63 Western J. of Communication 3, 382–83 (1999).

[9] *Primer, supra* note 5, at 8-9

Figure 1 - Flowchart of a Website Request

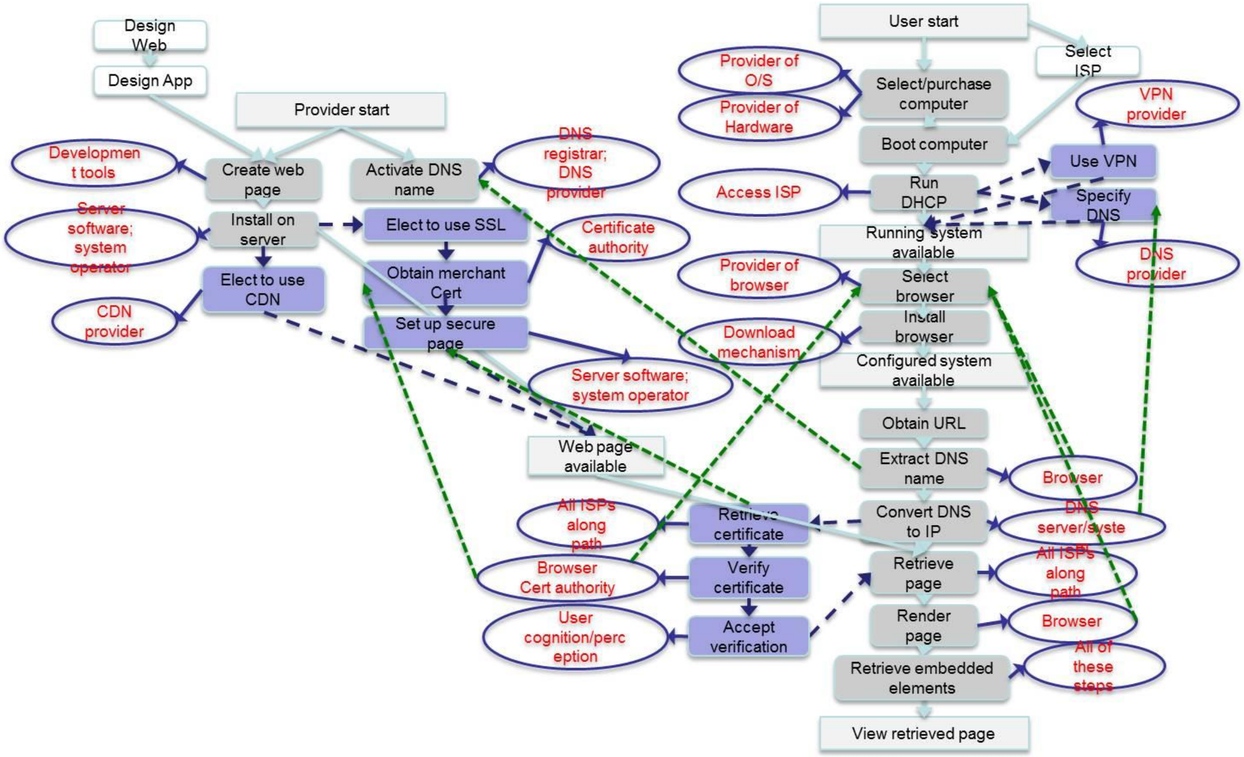

Figure 1 from *Primer, supra* note 5, at 39.

In all, this chart describes dozens of individual steps that must be satisfied by such diverse pieces of technology as the user's browser, the Internet Service Provider's infrastructure, the server hosting the site, and many others, before a website can be displayed. In other words, if any of these numerous steps fail, the user who requested the website will receive an error message instead of the desired content. Misconfigurations, coding errors, and unforeseen issues with the technology itself also may result in a failure. In addition, malicious actors may use each of these steps as a potential attack vector in order to carry out a cyberattack.

While Figure 1 is specific to the act of requesting a web page, this level of complexity exists in every piece of information technology and in every communication facilitated by the Internet. This is due to the fact that the Internet is a massively complex, highly distributed system of systems. At a fundamental level, the Internet is a not a singular "whole," but a web of individual pieces of information technology that are connected by communication protocols. Every device that connects to this web – smartphones, servers, Internet-enabled refrigerators, etc. – is itself a highly complex system of interacting information technology components. In such a system with complex communication protocols, there is a high probability that there are weaknesses that can be used to compromise the reliability or security of that system. When billions of devices are connected together into a distributed network, as they are in the Internet, that probability scales exponentially.

The Fundamental Nature of the Internet Creates an Asymmetric Threat

The fact that the Internet is an open system with many interconnections makes it especially vulnerable to disruption. Furthermore, this vulnerability is asymmetrical: the individual intending to compromise a system can do so at little cost and with little risk of being caught, while the costs of defense, as well as potential consequences, can be large. In other words, a malicious actor need only be in possession of a working Internet connection and an exploitable vulnerability in a target information system in order to compromise it. In addition, the global scale and complexity of cyberspace provide malicious actors the flexibility and relative anonymity to identify or craft an attack that fulfills their objective with minimal fear of consequence. There is also little to no cost for failure. They simply try again and again. Attribution of cyberattacks remains incredibly difficult, and even in cases where cyber "criminals" are indicted, the legal framework prosecuting such cybercrimes remains ill-defined, immature, and bound by geographical borders that do not exist in cyberspace.

Conversely, those responsible for defending information systems must simultaneously keep pace with a wide variety of threats and guard against all possible weaknesses to avoid a breach. This is difficult from a pragmatic perspective – consider Figure 1 and the dozens of steps it takes to view a website, each of which may be vulnerable to attack. In addition, given the low cost, the low risk of consequence, the range of actors and motivations, and the ever expanding scope of vulnerabilities, cyber threats evolve at a rapid pace. This makes it increasingly difficult to identify and eliminate vulnerabilities or malicious actors. A number of recent reports illustrate this challenge:

- Cloud security company Panda Security recorded 15 million new malware samples in the second quarter of 2014, an average of 160,000 new samples every day;[10]

- The PricewaterhouseCoopers (PWC) *Global State of Information Security Survey (GSISS) 2015* report stated that the total number of security incidents detected by survey respondents increased 48 percent from 2013 to 42.8 million, or 117,339 incoming attacks a day;[11]

- Mandiant's *M-Trends 2015* report revealed that approximately 70 percent of victims learned of their breach from an outside source, such as law enforcement. In addition, the report observed that, in 2014, the median number of days that a malicious actor persisted on a system prior to discovery was 205 days.[12]

These challenges are compounded by the numerous avenues for entry available to attackers. For example, malicious actors develop credible looking emails containing a link infected with malware. If an employee inside an organization clicks that link, the attacker has

[10] PANDA LABS, Q2 REPORT 2014, *available at* http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Informe-Trimestral-Q2-2014-EN.pdf.

[11] PWC, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD: KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2015, *available at* http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml. [Hereinafter, *PWC*]

[12] MANDIANT, A FIREEYE COMPANY, M-TRENDS 2015 THREAT REPORT, *available at* https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html.

gained entry. Attackers also can take advantage of weaknesses in the supply chain. They can gain entry to a larger organization by targeting a vendor with weaker security, especially small and medium sized companies, which typically have fewer resources to devote to security.[13]

The issue of cost is not limited to small and medium-sized companies. Cybersecurity is incredibly expensive. According to PWC's survey, organizations budgeted an average of $4.1 million for 2014 for information security.[14] In that same year, cybercrime cost organizations on average $7.6 million globally, and $12.7 million in the U.S.[15] The true costs of cybercrime are difficult to pinpoint given the complexities of calculating the value of lost intellectual property, reputational damage, delays to innovation, etc.[16] In addition, some estimates suggest that more than 70 percent of breaches go undetected.[17]

The complexity of the Internet and cyberspace, the weaknesses that are inherent in that complexity, and the asymmetric cost-benefit between malicious actors and defenders together will make it difficult, if not impossible, to spend, train, or "solve" our way out of cybersecurity problems. The technologies are too complicated, too dynamic, and too diverse. Reliability and security weaknesses exist as part of the Internet ecosystem, and the pace of innovation and adoption of new technologies ensures that new weaknesses will continue to be created and introduced. As our dependence on these technologies increases and they become entwined in everything we do, cyberspace provides limitless and adaptive attack surface.

Balancing Security Needs with Innovation, Convenience, and Usability

Cybersecurity has become a cost-benefit analysis. Governments, businesses, and individuals that depend on the Internet must make security decisions based on their own security, economic, and personal preferences. Improved security means higher costs, longer development timelines, and reduced convenience to consumers. In the current fast-paced, competitive information technology market, each of these factors undermines the economic prospects of a product, service, or business. Further, given the nature of the Internet, the complexity of information technology, and the existence of malicious actors in cyberspace, there is no assurance that a security improvement will be effective. At the same time, failure to provide adequate security can result in grave economic consequences, including but not limited to financial penalties, loss of intellectual property, and lost consumer confidence.

In light of recent, large-scale cyber-attacks, there is renewed interest in developing "solutions" to the cyber threat. While there are opportunities to improve the nation's ability to detect, defend, respond to, and recover from cyber-attacks, it is important not to undermine the benefits of cyberspace. In evaluating potential security measures, government, businesses, and

[13] *PWC*, *supra* note 11, at 8.
[14] *PWC*, *supra* note 11, at 20.
[15] PONEMON INSTITUTE, 2014 GLOBAL REPORT ON THE COST OF CYBER CRIME, *available at* http://h20195.www2.hp.com/v2/getpdf.aspx/4AA5-5207ENW.pdf?ver=1.0.
[16] *PWC*, *supra* note 11, at 11.
[17] *PWC*, *supra* note 11, at 8.

individuals must consider the costs relative to the benefits and the impact on expectations for cost, convenience, privacy, and civil liberties.

C. **Looking Ahead**

Our daily routines rely on information technologies connected to and dependent upon the Internet and cyberspace. Today, a handheld mobile device can start our cars, unlock our homes, make credit card payments, and monitor our health. A refrigerator can tell us when we are low on milk. We can access Twitter from our outdoor grills. These Internet-enabled devices collectively are referred to as the "Internet of Things," and hardware networking company Cisco believes that they will become so prevalent that by 2020, the number of devices connected to the Internet will exceed 50 billion.[18]

A report by the Institute of Electrical and Electronics Engineers Computer Society (IEEE CS) entitled *IEEE CS 2022* takes that prediction one step farther. The report first states, "[a]s a result of [the] pervasive penetration of computing and communications capabilities, human knowledge, intelligence, and connectivity are increasingly enhanced and augmented by information technology."[19] The IEEE CS then predicts a society that is so embedded with Internet-enabled devices that society's interactions with information technology and the Internet will become so automatic and transparent in daily life that it will create a world of "seamless intelligence."[20] The executive chairman of Google recently provided a similar assessment – eventually, the Internet will become so closely entwined with our daily lives that, to our perception, it "will disappear."[21]

Modern society has become so integrated with information technology and the Internet that cyberspace is no longer simply a place we visit, but a place we live. Through our social media profiles, our bank accounts, our digital health records, and even our browsing histories, we create virtual identities and entrust those identities to cyberspace. Therefore, it is important to examine the benefits and risks of increased integration with information technology, the Internet, and cyberspace.

V. **ISSUES**

The following issues may be examined at the hearing:

- How the challenge of cybersecurity is inexorably connected to the history and structure of the internet;
- The economic, social, and cultural factors that contribute to the challenge of cybersecurity;

[18] DAVE EVANS, CISCO, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[19] HASAN ALKHATIB ET AL., IEEE COMPUTER SOCIETY, 2022 REPORT (2014), *available at* http://www.computer.org/cms/Computer.org/ComputingNow/2022Report.pdf.

[20] *Id.*

[21] Georg Szalai, *Google Chairman Eric Schmidt: "The Internet Will Disappear,"* THE HOLLYWOOD REPORTER, Jan. 22, 2015, *available at* http://www.hollywoodreporter.com/news/google-chairman-eric-schmidt-internet-765989.

- The tradeoffs associated with effective security;
- Why there is no immediate solution to the cyber threat;
- The importance of cybersecurity to commerce and the economy in the 21st century;
- Current trends and emerging threats; and,
- Expected advancements in technology and their relationship to cybersecurity.

VI. **STAFF CONTACTS**

If you have any questions regarding this hearing, please contact John Ohly or Jessica Wilkerson with the Committee staff at (202) 225-2927.