Prepared Statement of
Anthony J. Ferrante
Senior Managing Director and Global Head of Cybersecurity
FTI Consulting
Before
The U.S.-China Economic and Security Review Commission

Hearing on China, the United States, and Next Generation Connectivity

Thursday, March 8, 2018
2255 Rayburn House Office Building
Washington, DC 20515

Chairman Cleveland, Vice Chairman Bartholomew, and Commissioners, thank you very much for the opportunity to testify today on a very important issue.

My name is Anthony J. Ferrante, and I am a Senior Managing Director and the Global Head of Cybersecurity at FTI Consulting, a global advisory firm. I focus on cybersecurity resilience, prevention, response, remediation, and recovery services. Over the last 15 years, I have provided incident response and preparedness planning to more than 1,000 private sector and government organizations, including over 175 Fortune 500 companies and 70 Fortune 100 companies.

Before joining FTI, I served as Director for Cyber Incident Response for the United States National Security Council at the White House, where I regularly coordinated responses to domestic and international cybersecurity incidents. I also led the development and implementation of Presidential Policy Directive 41, the United States government's key policy guiding cyber incident response efforts. Before joining the National Security Council, I spent several years in the Federal Bureau of Investigation's (FBI) Cyber Division. I was on the FBI's Cyber Action Team, which deploys around the world to respond to the most critical cyber incidents on behalf of the United States government, and I eventually became Chief of Staff of the FBI's Cyber Division. I also served as an Adjunct Professor of Computer Science at my alma mater, Fordham University, where I founded the International Conference on Cyber Security in 2007.

I'm extremely pleased that the Commission has taken an interest in such a crucial area for both the future of United States businesses and citizens as well as the safety of our nation overall.

Today, I want to talk about the significant wave of innovation that has overtaken the world in the last few decades, both the benefits and risks associated with new technologies, and what businesses and governments are doing to respond to these risks. In closing, I would like to share a few recommendations in terms of how we can be doing more to safeguard our society.

The Global Race to Innovate

In today's tech-driven society, countries recognize the key to economic well-being and overall security is their ability to innovate. Successful businesses are keenly aware of this fact, and governments are focused on creating advantageous environments where companies are incentivized to invest in technology. In addition to domestic growth, companies are encouraged to invest abroad through joint ventures and acquisitions in order to gain access to new market share and critical technologies.

Without a doubt, the focus on technological innovation has been wildly successful. As a result, high-quality devices have become available to broader populations at cheaper prices. Cell phones are a perfect example. In 2002, a little over half of adults had cell phones - today, 95% of adults have them.[1] It's crucial to remember that these devices, and the many others that now power our daily lives, require Internet connectivity. Today's refrigerators, cars, and even buildings are connected to the Internet. It's estimated that more than 200 billion Internet-connected devices will be in use around the world by 2020.[2]

In order for these devices to communicate effectively, networks are continually growing in scope and speed to support this unprecedented level of connectivity. A look back at past generation networks shows the massive leaps we've made in order to support our increasingly tech-driven world. 2G networks were designed for voice, 3G networks were designed for voice and data, 4G networks were designed for broadband Internet experiences, and now 5G networks are being developed to fuse computing capabilities with communications in real time.[3] The speed at which these improvements have occurred is staggering. Already, companies and countries alike are exploring the implementation of advanced 5G networks.[4] There's no reason to think that this breakneck pace will slow, and before long we will be talking about 6G, 10G, or even later generation networks. These networks will support a fundamental platform for new services and applications in tomorrow's economy, such as public safety, intelligence transportation, smart grid management, and mobile applications – all of which are integral to our national security and economic prosperity. This ever-increasing level of connectivity, often referred to as the Internet of Things (IoT), is the future, and the benefits are felt across the board.

The Benefits of IoT

IoT Strengthens our National Defense: Our forces' command centers traditionally relied on troops on the ground and aerial intelligence to communicate pertinent details on areas of operation. With new IoT technology, command centers collect data from devices, sensors, and cameras—mounted on unmanned vehicles, like drones, manned vehicles, soldiers, and

[1] http://www.pewInternet.org/fact-sheet/mobile/

[2] https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png

[3] https://qz.com/179980/the-plans-for-5g-to-power-the-Internet-of-things/

[4] http://www2.itif.org/2016-5g-next-generation.pdf

weaponry— enabling them to develop comprehensive battlefield situational awareness in real time.[5] Such intelligence helps our forces achieve objectives and minimize casualties.

IoT Unlocks Efficiencies for Businesses: When running large infrastructures or equipment, such as oil rigs, a malfunction or mishap can cost companies millions of dollars. To prevent this, oil companies closely monitor each small component of their rigs, doing their best to anticipate when maintenance is needed or if a part needs to be replaced. IoT technologies can now link information on these machine components to companies' repair departments and supply chains. Then, when a part is not working or appears to be failing, the appropriate personnel are notified, and they can carry out the necessary repairs. This predictive maintenance technology can save companies on personnel costs and minimize the risks of machine failure.[6]

IoT Brings Convenience to Consumers: Let's take a look at smart home technology. Currently, I can turn on the air conditioning system in my apartment with a simple voice command or with my smart phone, and our networks have the capability to support these interconnected devices. While these technologies have made our day-to-day lives easier, technological innovation is only going to take things a step further. Imagine driving home from work on a very hot summer day, and you have on a wearable device that recognizes your body temperature and sends the data to your phone—this is happening today. Once you reach a certain point in your commute, your phone recognizes your location and automatically sends a signal to your air conditioning system to power on. When you enter your home or apartment, it's the perfect temperature, and you did not have to press a button, open an application, anything.

The Risks Associated with IoT and 5G

While governments, businesses, and consumers are reaping the benefits of IoT technologies—particularly the significant amounts of data that enable the development of new technologies—increased interconnectivity, coupled with faster, more powerful networks, creates new vulnerabilities. Today, the biggest global cybersecurity threat derives from IoT technologies. Governments, businesses, and consumers have eagerly incorporated these devices into their daily activities. But they usually do so without even baseline security measures, such as changing the factory setting passwords on these devices. Unfortunately, this lax, plug-and-play culture makes us far more susceptible to cyberattacks.

The best analogy I can think of is the example of automobiles in the United States. Automobiles are everywhere. Almost every household has at least one and businesses of all sizes utilize vehicles – we're talking anything from a small pizza shop using a single car for deliveries to distributors operating huge fleets. But the drivers in these vehicles all operate within relatively well-established "rules of the road." When people get in their cars, they know that the brakes need to be functioning or that seat belts need to be on; they know that they drive on the right

[5] http://www.windriver.com.cn/downloads/whitepaper/wind-river_IoT-in-Defense_white-paper.pdf
[6] http://www.digitalistmag.com/iot/2017/05/08/5-real-business-uses-of-internet-of-things-05072303

side of the road or need to use their blinkers when they shift lanes. It's not a perfect system, but it's also not total chaos.

But we can't say the same for the IoT technologies. The proliferation of these devices and the development of these complex networks has been so fast, and the devices so easy to use, that there has been no time to take a step back and establish foundational "rules of the road." People don't change the password default settings on their devices; they don't pay attention to the ways they are streaming data; they don't take care when storing personal or sensitive information on different devices. The same is true of businesses. And without those underlying "rules of the road," vulnerabilities start to open up which can and have been exploited.

With the current trend, this problem is only going to become more pronounced. Again, these networks are developing at a breakneck pace, as are the devices we are using on them. The longer we go without a culture shift that emphasizes safety and preparedness, for governments, businesses, and consumers alike, the harder it will be to instill order and maintain safe networks. We're already seeing the consequences with the level of exposure our networks have to attacks. And not only are we becoming more vulnerable to attacks, but the tools used by malicious actors are becoming more effective and widely available. By 2019, the cost of data breaches to companies will reach $2.1 trillion globally, increasing nearly four times the estimated cost in 2015.[7] To meet these threats, 85% of organizations are considering, exploring or implementing an IoT strategy.[8] But while awareness is growing, concrete steps to improve preparedness and response have lagged behind.

In order to accurately assess our risk vulnerability, it is important to know where the threats are coming from and in what form. Rogue actors are certainly something that we need to be mindful of. But nation-states—like China, Russia, Iran, and North Korea— are becoming increasingly advanced and sophisticated in their abilities to engage in malicious cyber activity. Most importantly, they have shown a willingness, and in many cases a preference, to use cyber aggression as a tool due to relatively low operational costs and the ability to deny affiliation. As a result, the line between criminal and nation-state activity is becoming increasingly blurred.[9]

Types of Attacks - DDoS

Before delving into some contemporary examples, I wanted to touch very briefly on "distributed denial of service" (DDoS) attacks. Because of their simplicity and function, this specific type of attack provides a great example of how the addition of many IoT devices and stronger networks will increase the scope and scale of cyberattacks we face. With DDoS attacks, hackers use groups of Internet-connected devices, known as botnets, to overwhelm servers,

[7] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
[8] https://www.business.att.com/cybersecurity/archives/v2/iot/
[9] https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

websites, and networks. Essentially, the devices are used to spam networks with so much traffic that they shut down.

These DDoS attacks are the blunt tools of cyberattacks – they don't attempt to infiltrate or steal data and sensitive information. Instead, they use brute force to disrupt whole portions of networks. Nevertheless, these can be incredibly disruptive attacks. Some have shut down websites or smaller servers used by banks or other critical businesses. Others have been so large that they've crippled entire networks. Crucially, DDoS attacks utilize the insecure and unprotected devices in the IoT to carry out these attacks. Thus, electronic devices that have become part of our everyday lives can be coopted and used for nefarious purposes by malicious actors. Ultimately, more unsecured devices coming online will result in larger, more expansive botnets, and powerful networks—whether it be 5G now, or 8G five years from now—which will create additional, and faster, avenues for hackers to exploit.

Rogue Actors

Cyberattacks from rogue actors pose a serious threat and can have major implications for millions of unsuspected individuals. Take, for example, a cyberattack in October 2016, where hackers targeted a domain provider company, Dyn, and subsequently disrupted a broad array of the Internet's biggest websites, such as Twitter, Netflix, Reddit, and CNN. This DDoS attack exploited the weak security of devices in the IoT to introduce malicious software called Mirai. These devices were only protected by factory default, out-of-the-box security measures and were thus easily accessed and corrupted by the software. The software exploited these "soft targets," which are designed so owners can simply plug in and use them immediately. Again, many people don't even consider applying security updates or advanced settings. Their top priority is simply using the new device.

While the identity of the perpetrators of this particular attack has still not been confirmed, it's believed that it was not the work of a nation-state sponsored group, as multiple hacktivist groups claimed responsibility for the attack. One article even alleged that the attack was perpetrated by a "single very angry gamer."[10] Regardless, the Dyn attack highlights our vulnerabilities and the scope of the threats we need to be prepared for. The malicious software preyed upon everyday devices that are a part of the IoT. And the source code for the software, the actual tool itself that the attackers used, had been made publicly available on the Internet just a few weeks prior to the attack.[11] Even more troubling is the fact that our vulnerabilities are expanding at a rapid pace. As 5G and later generation networks come online and as the IoT grows, it is likely that the overall frequency of attacks, and the intensity of individual attacks themselves, will only increase.

[10] https://www.forbes.com/sites/leemathews/2016/11/17/angry-gamer-blamed-for-most-devastating-ddos-of-2016/#8bb93a42dac6

[11] https://www.eyerys.com/articles/timeline/ddos-dyndns-Internet-breaks#event-a-href-articles-timeline-facebook-and-billion-userfacebook-and-a-billion-user-a

Nation-States

Perhaps the greatest cyber threat comes from organized actors, often "countries of concern" that seek to gain access to sensitive information about the United States and its citizens. For example, in September 2012, massive DDoS attacks were carried out against dozens of large banks, including Bank of America, JPMorgan Chase, Wells Fargo, US Bank and PNC Bank, shutting down their websites for extended periods of time.[12] At the time, the volume of traffic was 10-20 times the volume seen in standard DDoS attacks. Numerous groups claimed responsibility, but it was ultimately determined that Iran had sponsored the attacks.[13] And last year, a grand jury in New York indicted seven Iranian individuals—who were employed by two Iran-based companies, ITSecTeam and Mersad Company, both of which were sponsored by Iran's Islamic Revolutionary Guard Corps—for carrying out the largescale DDoS attack.[14]

The event illustrated the ease with which nation-states can use their resources to conduct large-scale attacks against the United States. Despite the fact that the United States was spending $3 billion on cyber defenses at the time, $2 billion more than Iran, we were unable to defend ourselves from the attack, thus crippling our financial services industry. Experts have indicated that the attack marked a shift in Iran's cyber policy which emphasizes offensive capabilities and exploits the myriad of vulnerable targets available in the United States.[15]

In another example, in February of 2014 employees of a subsidiary of Anthem, the health insurance giant, received phishing emails. These are designed to appear as normal emails, but instead give malicious actors access to company networks. [16] One unknowing employee opened the email, giving a hacker remote access to the computer. This allowed the hacker to gain access to Anthem's core systems. The hacker then continued to operate within the system for approximately a year, exploring ways to retrieve sensitive information.[17] Ultimately, in February 2015, Anthem announced that the information of 78.8 million individuals (both customers and employees) had been compromised in a large-scale cyber incident.[18]

Though unconfirmed, the hackers are believed to be a part of China's military cyber-espionage division.[19] Experts suggest that the evidence, such as IP addresses and email accounts, indicate that China was behind the attack.[20] This is a perfect example of how nation-states can use to tip the balance in their favor. For the low price of outfitting a small cyber strike force, China gained access to the healthcare information of millions of Americans. This information could give a

[12] http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html

[13] https://www.cnn.com/2012/10/15/world/iran-cyber/index.html

[14] https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

[15] https://www.wsj.com/articles/SB10000872396390444657804578052931555576700

[16] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

[17] https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

[18] http://www.insurance.ca.gov/0400-news/0100-press-releases/2017/release001-17.cfm

[19] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

[20] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

competitive edge to China's biotechnology industry.[21] And this is just one incident. There are opportunities for nation-states to replicate such attacks across all American industries.

Response

How Businesses Are Responding

The scope of vulnerabilities and threats posed by these expanding networks has generally exceeded the ability and willingness of businesses to respond to them. The fact is that the combination of automation, machine learning, artificial intelligence, digitized supply chain management and communication technologies create massive vulnerabilities for all businesses. According to a recent study, cyber incidents are at an all-time high, with 86% of the companies surveyed saying they experienced at least one cyber incident.[22]

And it's not only the business operations that pose a threat – individual employees also present an opportunity for malicious actors to gain entry. For example, thousands of executives are targeted by cyber actors every day.

Unfortunately, the response to these threats has been weak. Businesses continue to operate with a large gap between their information technology (IT), security departments, and their core business functions. Failure to integrate cybersecurity into daily operations drastically reduces business' ability to defend and respond to cyber threats and incidents. Essentially, they are failing to both fortify their networks and to effectively manage breaches once they occur.

Further, an unwillingness to accurately report on cybersecurity status exacerbates the issue. There is often a habit of hush-hush management and underreporting of incidents across the board, from retail businesses, which store customer information, to utility companies that provide the power necessary for our nation to function on a daily basis. This opacity is a real problem because it conceals the ubiquitous nature of the threat we face. I don't think individual businesses or the public understand the scope of these vulnerabilities, and without that knowledge there is no impetus to develop the necessary defenses. We need to work towards a culture shift that incentivizes and rewards businesses to report breaches, communicate with each other, and coordinate responses.

How the Government is Responding

Thankfully, the United States government is showing signs that it recognizes the need for action and collaboration, as evidenced by today's hearing. And this recognition and subsequent discussions are already showing early signs of coercing the government to take action. For example, in the wake of several large cyberattacks, President Donald Trump issued an Executive

[21] https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

[22] https://www.prnewswire.com/news-releases/businesses-report-all-time-high-levels-of-fraud-cyber-and-security-incidents-during-2017-300585657.html

Order in May of 2017 calling for the Departments of Commerce and Homeland Security to identify and promote action to reduce cyber threats. Last month, Commerce and Homeland Security released a preliminary report, which included a series of goals to reduce the threat of automated, distributed cyberattacks and focused on the need for collaboration among stakeholders—including business executives, thought leaders, and elected officials—to combat new cyber threats.[23]

The Administration's FY19 Budget Request called for $80 billion in IT and cybersecurity funding ($45.8 billion for civilian agencies), representing a 5.2% increase from last year.[24]

The Administration is not alone in its efforts to mitigate these threats; Congress has increased government funding for cyber initiatives. Between 2007 and 2016, spending on unclassified programs to combat cyber threats rose from an estimated $7.5 billion to $28 billion.[25] In 2016 the Defense Department spent $18.5 billion in cyber-related efforts, nearly 30% above the prior year; Homeland Security spent $1.7 billion, a 9% increase; and Treasury spent $2.8 billion, a 42.7% increase.[26]

Such measures and funding are a good first step in guarding against the use of strategic legal investments. But we must also be vigilant in guarding against nation-state actors using illegal tactics to gain access to United States technologies and information.

Recommendations and Conclusion

1. We cannot operate in a bubble. The reality is cyber warfare and cyberattacks are not a United States problem, but rather a global one. With no existing "cyber norms," we have an opportunity to set the standards for 5G networks and IoT devices, where other nations will then follow suit. When it comes to cybersecurity, the adage "a chain is only as strong as its weakest link" certainly holds true. But the potential to begin a culture-shift in the approach to cybersecurity and the willingness to do so are two very different things. The United States government and businesses need to take concrete steps to lead by example and address cyber threats.

2. We need to help Internet service providers (ISPs) protect the end users – United States businesses, consumers, and the American people. ISPs are the first line of defense in both identifying and mitigating cyberattacks. If I were to use an analogy to describe ISPs, they would be the state troopers, with highways serving as the networks. In order for state troopers (ISPs) to guard against risky activities on highways (networks), they need proper resources. And, with highways getting even larger as a result of increased traffic

[23] https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf
[24] https://www.whitehouse.gov/wp-content/uploads/2018/02/FY19-Budget-Fact-Sheet_Modernizing-Government.pdf
[25] http://www.thefiscaltimes.com/2017/08/06/US-Spends-Billions-Cybersecurity-No-One-Sure-Exactly-How-Much
[26] http://www.thefiscaltimes.com/2017/08/06/US-Spends-Billions-Cybersecurity-No-One-Sure-Exactly-How-Much

(more IoT devices), we need to ensure state troopers have the necessary resources to prevent malicious actors from harming the end users.

3. We need to invest in cyber education. This is absolutely crucial. Of course, we need to ensure that the current everyday consumers recognize the vast risks associated with IoT devices and are armed with an understanding of how to contribute to overall security. But we also need to take the long view and invest in educating teenagers and young minds charged with developing our future software and technology. These generations are going to grow up with this technology, and given the pace of technological improvements we need to assume that their lives will be much more tech-centered than has been the case in the past. It is our responsibility to arm our younger generations with an understanding and appreciation for the potential threats an interconnected, IoT-driven world will present. An underlying culture shift in cybersecurity awareness must be fully integrated into future developments as new generations write code, invent new devices and improve network capabilities.

4. We need to educate the public about cyber threats. As I previously mentioned, individuals have greatly benefited from innovative new devices, many of which are connected to the Internet. While we should celebrate these advances, people must understand that these devices can serve as a pathway for uninvited cyber criminals to enter their homes. Beyond simply understanding that the threat is real, the government and industry leaders should continue to play an important role in educating the public about ways in which they can mitigate the risk of cyber attacks