PREPARED STATEMENT OF KEVIN MANDIA, CEO, FIREEYE, INC.,

SENATE HOMELAND SECURITY & GOVERNMENTAL AFFAIRS COMMITTEE

Evolving Threats to the Homeland

SEPTEMBER 13, 2018

Mr. Chairman, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to share FireEye's perspective regarding cyber threats to the United States of America.

Before I begin discussing cyber threats, I would like to take a moment to extend our condolences to each of you for the loss of your dear friend and colleague, Senator John McCain. His distinguished service in the U.S. Navy and in Congress was an inspiration to us all. He represented Americans, and he represented the best of American values.

My testimony today is derived from FireEye's unique visibility and experience responding to significant breaches around the globe, from the intelligence collected and produced by our cyber threat analysts, and from the products our customers use to detect intrusions and respond to attacks. I intend to discuss the cyber threats to our nation, what their impact could be, and some of the major actions we could take to prepare for these threats.

Introduction

I have been working in cybersecurity for more than 20 years, since I was first stationed at the Pentagon as a Computer Security Officer for the United States Air Force, and later as a Special Agent in the Air Force Office of Special Investigations, investigating computer intrusions into our military networks. My entire career has been dedicated to cyber security, and I have had the honor of serving as FireEye's CEO since 2016.

FireEye is on the front lines of the cyber conflict every day. We have over 100 threat analysts, in 18 different countries, covering 32 different languages, tracking cyber attackers. We have over 300 security experts, working in 26 countries, investigating successful network intrusions. We review over 1 million new malware samples everyday, and we have over 15 thousand global sensors - detecting anywhere from 50 thousand to 70 thousand malicious events per hour.

Today, through a shared services contract with DHS, more than 100 departments and agencies are using FireEye Threat Intelligence in their security operations. We collect, prepare, and disseminate intelligence on cyber threats daily, and the discussion I can share today is only a fraction of the intelligence we have accumulated.

The Threats to the United States

Let me begin by sharing three general observations about cyber threats to the United States.

First, I believe the United States is uniquely more vulnerable in cyberspace than other nations. We are a lot more dependent on the Internet, technology and network infrastructure than the nations that host the most prevalent cyber attackers. Second, much of our critical infrastructure is privately rather than publicly owned, requiring more private/public partnership to defend our infrastructure. Finally, our freedom of the press – a foundational ingredient of our democracy – allows adversaries to achieve two types of attacks that are far less impactful in closed societies – the ability to conduct influence operations on the American public – and the ability to release or threaten the release of private information stolen in the latest data breach as leverage to elicit some behavior.

Second, while public discussion about cyber attacks frequently focuses on "Cyber Pearl Harbor" scenarios, I believe that our nation is more likely to face an enduring, more protracted cyber campaign akin to "cyber trench-warfare."

1 – The first characteristic of cyber trench warfare is that it will likely be conducted below the threshold of actions that might elicit a formal, aggressive response by the United States.

2 – Second, these campaigns will be long-term, resource-draining cyber operations.

3 – Third, they will target the whole-of-society rather than just military and government networks, seeking to wear down our morale, trust, and readiness without resorting to a single, game-changing attack. Looking back on my experiences in both the military and in the private sector, it is clear to me that our nation's greatest vulnerabilities are not the defense and military networks or the large critical infrastructure providers. Instead it is the targeting of everyday Americans and their businesses. These softer targets, such as individuals, state and local governments, public schools, academia, smaller businesses, form the fabric of our daily lives. Not every company or organization has the resources or capabilities to defend itself in cyberspace, and a catastrophic or even gradual failure of the softer targets will result in significant impact perhaps as grave as attacks against well protected, critical systems.

4 – And lastly, Cyber trench warfare will have a persistent negative economic impact.

Based on these qualities, there are some security experts who would opine that we are already engaged in "cyber-trench warfare" today.

My last general observation is that any of the damage from cyber conflict easily spreads to impact many facets of our daily lives – and the impact will continue to grow as we live more connected. We refer to this widening impact as the "butterfly effect." The most poorly defended businesses might be the ones most targeted, and certainly the one's most impacted during a cyber conflict, and the impact would permeate our daily activities in ways that can be difficult to predict.

Now I would like to discuss some specific threats to our nation that we ought to prepare for.

The Threat to Utilities

American utilities will likely be targeted during any future armed conflict and would also be prized targets to groups or lone actors with malign intent.

At FireEye, we have seen the targeting of critical infrastructure in the Middle East, where adversaries disrupted the safety systems of a utility provider. In Ukraine, we observed attacks on the electrical grid, disrupting businesses and homes across the country. We alerted the public to North Korean spear-phishing attacks of U.S. electric companies late last year, as threat actors attempted to manipulate workers into clicking on illicit emails.

While most large-scale utility companies have complex redundancies to protect against large-scale disruption, smaller utility providers may be less-equipped to defend against nation-state level cyber activity. It has been our opinion, while the bigger, well-resourced utilities may operate through an advanced cyber attack, the less resourced, more rural utilities are at a higher risk of failure. Therefore, the probable impact of a sophisticated, prolonged cyber attack against American utilities will have far more negative impact on the vital services in rural areas and smaller municipalities than in the major cities.

The Threat of Indiscriminate Attacks

The United States can expect future attacks that are indiscriminate, seeking to effect as many citizens as possible at once. These attacks would be intended to disrupt business as well as personal endeavors and would have wide-ranging impact.

For example, North Korean actors used ransomware to conducted anonymous mass extortion to obtain crypto currency. Other nations will likely adopt this tactic for political ends. Attacks like these can also be financially destructive; June 2017's NotPetya ransomware attack caused approximately $10 billion worth of damage, according to government estimates.

As a hypothetical, one can imagine a nation wanting to compel a response of some kind from another nation. Instead of using military force or economic sanctions, it could choose to release ransomware targeting that country's citizens, critical

infrastructure, and government functions – not returning the use of encrypted data being held for ransom until the desired response is taken. With the anonymity of the Internet, nations could spread doubt by claiming such an attack was the work of cyber criminals and hold entire nations hostage with limited risk or repercussions. This scenario is notional, but ransomware's capability to have widespread impact and its reversibility make it likely to be deployed in the coming years for strategic gains.

The Threat of Information Operations

We have heard about Russian Information Operations, but the number of nations leveraging social platforms and incorporate today's technologies are expanding. Just two weeks ago FireEye announced the discovery of an Iranian influence campaign extending from the Middle East to Europe and the Americas.

Information operations are likely to be a persistent force in media and society from now on. The evolution of information operations allows Nations to individualize their efforts, and to be informed person-by-person by our likes, shares, and other information freely available on social media.

Artificial intelligence will add to the effectiveness of these information operations. Nations will be able to draw on massive data sources of information to curate content tailored to the characteristics of each user. AI is also giving rise to entirely new threats, such as deep fakes— or counterfeit content so realistic that we may soon no longer be able to trust that a video we see, or a sound bite we hear, is authentic.

What the U.S. Can Do to Prepare for These Threats

There are many actions the United States Government and the private sector can do to help mitigate the impact of these threats, and today I would like to mention a few of these actions. We should accelerate a coordinated defense against the cyber threats to our nation by promoting a system that fosters actionable and timely information sharing, supports the practice of resiliency in businesses, secures the supply chain, and identifies and holds perpetrators of cyber-crime or cyber trench-warfare accountable.

Information Sharing

The sharing of actionable threat information will narrow the security gap facing businesses and organizations today. Government, including law enforcement, and some companies have this actionable intelligence. We need to create a way in which they can share this information in a standard, codified, machine-readable way that does not betray or diminish the effectiveness of our national security or law enforcement missions, or significantly impact our privacy and civil rights. If we do it

right, sharing threat information will promote an aggressive, dynamic "learning system" of cyber-security for the nation. Effective information sharing:

1 – Acts as an early warning system giving potential victims advance notice of significant threats;
2 – Promotes technologies that facilitate the effective use of threat information;
3 – Empowers the private sector to defend itself more effectively; and
4 – Significantly reduces the duration and impact of breaches, should they occur.

The private sector cannot do this alone. Our nation must find ways to unite the American people and their businesses in a common defense alongside federal, state, and local network defense missions and to combine efforts with our allies in Europe, Asia, and the Middle East.

Promote Resiliency

As a country we also need to start thinking more about cyber resilience. Can major commercial enterprises continue to function if some or all of their internet-connected systems are disabled? Can the military deploy and command troops? What about the civilian government?

Few companies can adequately predict all the business operations or processes that are impacted by loss of Internet connectivity. I urge the Committee to consider ways it could require government agencies to develop and carry out continuity-of-operations plans that practice, even for just 24 hours, going without Internet connectivity while continuing critical functions. Private sector companies, too, would benefit from this model.

Strengthen Supply Chain Resilience

Threat actors have increasingly leveraged the trust between users and software providers. Users do not expect malicious code to be introduced by updates from trusted software vendors. In supply chain attacks, cyber threat groups target the build servers, update servers and other parts of the development or release environment. The hackers then inject malware into software releases, infecting users through official software distribution channels. This method allows attackers to target broad set of potential victims while obfuscating their intended targets.

In 2017, FireEye observed at least five cases where advanced threat actors compromised software companies to target users of the software. Chinese cyber espionage operators modified the software packages of a legitimate vendor, NetSarang Computer, allowing access to a broad range of industries and institutions that include financial services, transportation, telecommunications, energy, media, academic, retail, and gaming. Likewise, in June 2017, the NotPetya ransomware was spread to various European targets when Russian actors compromised Ukrainian

software vendor M.E.Doc. I am confident that advanced attackers will continue to leverage the software supply chain to conduct cyber espionage.

Hold the Perpetrators Accountable

Every day there is an onslaught of cyber attacks impacting American business and individuals. The largest contributor to the rising occurrence of these cyber attacks is that there are no risks or repercussions for those who commit them. Adversaries now believe they can attack our economy, our way of life, and our continuity of government without provoking a military response, so long as they do so in cyberspace. In short, there is no deterrence. Until we as a nation hold these threat actors accountable, we will likely continue to get sucker-punched in cyberspace.

Policymakers should continue diplomatic efforts to proactively define the rules of engagement with our international counterparts so that they expect a clear, consistent US response to each and every cyber attack. The agreement President Obama reached with President Xi in September 2015 to end cybertheft of commercial intellectual property between the U.S. and China led to significant decrease in operations stealing American intellectual property over the last few years. The effect this agreement had bringing adversary behavior in line with clear rules of engagement shows diplomacy can be an effective and enforceable means of peacefully improving America's cybersecurity.

Conclusion

The threats to our nation and to the world are growing, and we must be prepared to counter them. By establishing a system where the private and public sectors work together, practice together, and proactively use threat intelligence, America will build a dynamic cyber-defense system that grows smarter and more capable by the day. By exploring international rules of engagement and holding threat actors and the Nation's that harbor them accountable for their actions, the United States, and the daily lives of our citizens, will be safeguarded from the protracted cyber campaigns we are withstanding today.

Thank you very much, Mr. Chairman.