Hearing before the
House Armed Services Committee
"Cyber Operations Today: Preparing for 21st Century Challenges in an Information-Enabled Society"

April 11th 2018

The Honorable Michael Chertoff
Former Secretary of Homeland Security 2005-2009
Co-Founder and Executive Chairman, The Chertoff Group

Introduction

Chairman Thornberry, Ranking Member Washington, distinguished Members of the Committee, thank you for the invitation to discuss the current cybersecurity challenges and threats facing the homeland from Russia, China, and other nation-state actors and for providing me the opportunity to recommend ways to better prepare the government to face the challenges posed by advances in the cyber domain. I am pleased to join Secretary Jeh Johnson and General Keith Alexander who have both been prominent leaders on these issues.

The most recently-released 2018 Worldwide Threat Assessment published by the US Director of National Intelligence (DNI) warns that: "Competition among countries will increase in the coming year as major powers and regional aggressors exploit complex global trends while adjusting to new priorities in US foreign policy. The risk of interstate conflict, including among great powers, is higher than at any time since the end of the Cold War … Adversaries and malign actors will use all instruments of national power—including information and cyber means—to shape societies and markets, international rules and institutions, and international hot spots to their advantage."[1]

High-powered offensive tools are increasingly available to threat actors and have contributed to an uptick in cyber-attacks. Cyber-attacks are growing both in number and in sophistication and the scale of the theft of data has dramatically expanded in recent years. Broadly speaking, there are three categories of campaigns we see nation-states, to some degree or another, pushing. One is for intelligence purposes. The second issue is information operations designed to influence our institutions and societal norms. The third and most concerning dimension includes attacks that are designed to enable a military action or to threaten or carry out disruptive or destructive attacks.

Nation-states or state-sponsored actors will continue to use cyber means to gain advantage against the US from a political, financial, and military perspective. As noted in the World-Wide Threat Assessment, Russia will continue to attempt disruptive cyber operations with the intent to degrade democratic values as well as global alliances. Russia's wide range of operations include disruption of Ukrainian energy distribution networks, hack-and-leak influence operations, distributed denial-of-service attacks, and false flag operations. In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy. China will continue to view information warfare as military strategy and leverage cyber espionage to support its national security priorities. Cyber efforts from Russia, China, and other state-sponsored actors could have a detrimental impact on private companies, critical infrastructure, and our democratic institutions in the years to come.

[1] *See* https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

As I understand it, we have three Agencies responsible for defending against cyber-attacks: The Federal Bureau of Investigation (FBI) as the lead for law enforcement, the Department of Homeland Security (DHS) as the lead for critical infrastructure and defending government computer networks, and the Department of Defense (DOD) as the lead for defending the homeland, defending military computer networks, and developing and employing military cyber capabilities. There is no doubt that we have the capabilities necessary to counter and respond to the threats the US government faces from our adversaries. However, we must have a clearly defined strategy and develop policies to reflect that. In my testimony today, I will recommend ways for the US government to enhance our defenses through defining a cyber warfare doctrine that determines the level of attribution, simplifying information sharing programs between the public and private sectors, and incentivizing businesses to develop cybersecurity solutions to defend the homeland.

Understanding the current threat environment is essential if we are going to craft effective policy and defenses. I am therefore pleased to see the Committee's continued focus on this subject and appreciate the opportunity to provide my insights.

Data Theft for Intelligence Operations

A series of major thefts of personal data — not intellectual property — over recent years could suggest that a nation-state is trying to build a database of all Americans. This poses a threat to our national security because a nation-state could leverage this data for intelligence operations or influence campaigns.

- **OPM Hack:** The US Office of Personnel Management hack in 2014 was particularly worrisome. The White House said in 2015 that more than 21 million Social Security numbers, 1.1 million fingerprint records and 21.5 million forms with data like someone's mental-health history were stolen.[2] With technologies such as artificial intelligence, a hacker could generate useful information for intelligence operations from large sets of data. For example, a malicious actor could use the data to determine whether a corporate individual is really a government employee. The theft of fingerprints, as in the OPM attack, could also prevent government officials from going undercover in the future.

- **Yahoo Breach:** The recent Yahoo Breach is another example. Yahoo lost over 3 billion user accounts in two operations – one of which involved the engagement of two Russian Intelligence Officials[3]. The FSB, Russia's primary security service, allegedly hired the hackers to target US and Russian government officials, diplomats, military personnel, Russian journalists, financial sector employees and activists. The involvement of Russian spies suggests this was partly designed to aid espionage activities and is further evidence that the line between nation-states and criminal actors is becoming increasingly blurred.

Data Theft for Influence on Societal Norms

The Russians have weaponized the use of data to enhance and support their influence operations. In 2016, we saw an attack on the US Presidential election, an operation that the US Intelligence Community (IC) attributed to Russia. Russia also continued its influence operations in other countries of Europe. Ultimately, Putin's goal is to diminish the power and influence globally of the US and to shatter or splinter NATO.

- **Robert Mueller's Indictment:** A federal grand jury has indicted 13 Russian nationals and three Russian entities for alleged illegal interference in the 2016 presidential elections. The indictment says that a

[2] *See* https://www.opm.gov/cybersecurity/faqs/

[3] *See* http://fortune.com/2017/10/03/yahoo-breach-mail/

> Russian organization called the Internet Research Agency sought to wage "information warfare" against the United States and to "sow discord" in the American political system by using fictitious American personas and social media platforms and other Internet-based media. The indictment details an extremely sophisticated conspiracy in which defendants traveled to the United States to conduct research, employed specialists to fine-tune social media posts to "ensure they appeared authentic," and stole real people's identities to purchase online ads.

Russia will continue using propaganda, social media, false flag personas, and sympathetic spokesmen to build on its wide range of operations and exacerbate social and political issues in the US in 2018 and beyond. DHS and the IC must define a clear strategy to remedy this vulnerability. In his testimony in March, DNI Coats told Congress that the United States was “under attack” and yet there seems to be no strategy to combat this threat.[4]

Deterring a repeat of this conduct must be a priority for the entire US government, and indeed for all nations whose elections are susceptible to Russian interference. The need to impose costs is clear, but the challenge is to impose them in ways that matter to the Russian regime—not in ways that are projections of what would matter to the United States. Last week’s imposition of sanctions on 7 Russian oligarchs and 12 companies under their control was a good start.[5] However, we cannot rely on deterrence alone: we need to ensure the United States has capabilities on the shelf to prevent and preempt this kind of behavior ahead of the 2018 midterms, and we must make ourselves harder to hack by improving our defenses and becoming more resilient.

- **Election Security**: One tactical issue that Congress must take responsibility for is securing our electoral data. Chicago’s Board of Elections reported that names, addresses, dates of birth, and other sensitive information about the city’s 1.8 million registered voters had been exposed on an Amazon cloud server for an unknown period of time.[6] Worse, it appears that hackers might have gained access to employees’ personal accounts at Election Systems & Software, a major election technology vendor—information that could be used to hack a future US election. American elections are an increasingly easy target because our election technologies are antiquated and we have few federal level cybersecurity standards. An estimated 43 states rely on electronic voting or tabulation systems that are at least 10 years old. A survey of 274 election administrators in 28 states found most believed that their systems need upgrades. This is a matter of national security, and Congress should treat it as such. The $380 million in funding for election security that was included in the FY18 omnibus spending bill is a step in the right direction. The immediate funding will help states to replace outdated technology and improve cyber-defenses ahead of the 2018 and 2020 elections. A fair and safe election is one of the hallmarks of our democracy. While funding in the omnibus is an essential first step, it’s just that – a first step. Congress should take up the full Secure Elections Act without delay, so we can fully protect the security and integrity of our elections.

Data Theft for Disruption

We have seen the rise of disruption attacks over recent months. This is the most concerning type of attack as they could be designed to enable a military action or to advance a geopolitical struggle and they could have devastating impacts on our critical infrastructure.

[4] *See* https://www.usatoday.com/story/news/politics/2018/02/13/intelligence-director-coats-says-u-s-under-attack-putin-targeting-2018-elections/332566002/

[5] *See* https://home.treasury.gov/news/press-releases/sm0338

[6] *See* https://www.wsj.com/articles/congress-can-help-prevent-election-hacking-1504652957

- **Ransomware:** We've seen massive disruptions to business operations and municipalities through "ransomware," including episodes involving the WannaCry and NotPetya malwares. The most recent attack on Atlanta shut down government operations for over a week. The WannaCry attack ravaged computers at hospitals in England, universities in China, rail systems in Germany, even auto plants in Japan. Additionally, a large pharmaceutical company had 75,000 machines affected by the malware and lost critical research. Incidents like Atlanta, WannaCry, and NotPetya caused massive disruptions to enterprises and municipalities worldwide on an unprecedented scale and indicate a rise in nation-state actors involved in driving these kinds of attacks.

- **Ukraine:** In Ukraine, in 2016 and 2017, there were attacks on the country's energy infrastructure that caused the lights to go out. We've seen similar things in other parts of the world. The most concerning threat to national-security professionals is a devastating attack on critical infrastructure.

- **Russian malware found in critical infrastructure:** Similar to Ukraine, the Trump administration recently accused Russian government hackers of carrying out a deliberate, ongoing operation to penetrate vital US industries, including the energy grid — a major ratcheting up of tensions between the two countries over cybersecurity.[7]

- The Edison Electric Institute reported that its Federal government partners informed energy grid operators in North America of a threat targeting the energy and critical manufacturing sectors. While this incident did not have operational impacts, the group worked across the sector and with government partners to ensure the ongoing protection of the grid from this specific threat and from all cyber and physical security risks. Following the announcement of sanctions against Russian government cyber actors, the Electricity Information Sharing and Analysis Center (E-ISAC) provided potential indicators of compromise and other technical data to ensure electric companies in North America are prepared to protect and defend their networks. This information sharing is representative of the strong industry-government partnership, which exists through the Electricity Subsector Coordinating Council, and is vital to guarding the grid from all possible threats.

- Similarly, following the news of the intrusion, the Department of Energy created a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at the US Department of Energy (DOE). $96 million in funding for the office was included in President Trump's FY19 budget request to bolster DOE's efforts in cybersecurity and energy security.[8]

Responding to Today's Threats

Just as the threat environment has evolved, so too must our ability to respond to those threats. This evolution has been most evident within the intelligence community and military, where the National Security Agency (NSA) and United States Cyber Command continue to develop new capabilities designed to counter emerging cyber threats. While this is not the setting in which to focus on these capabilities, I can say that I am confident that the cyber capabilities of the United States are second-to-none. However, I believe there is still work to be done in other areas, particularly in regard to cyber strategy and policy outside of the military and intelligence communities. The two areas of strategy and policy I'd focus on most would be cyber defense and cyber deterrence.

[7] *See* https://www.us-cert.gov/ncas/alerts/TA18-074A
[8] See https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency

Cyber Defense

The first area of policy that I would address is in cyber defense. How we defend ourselves, and more particularly our cyber infrastructure and networks, is vital to our security and an area in which progress can have a direct impact on minimizing the harms of cyber-attacks. As many in the cybersecurity field have observed, an ounce of prevention is worth a pound of cure.

In order to improve our cyber defenses, it is important to understand how responsibilities for cyber defense are distributed. Within the Federal government these responsibilities are spread among several organizations, so there must be coordination and collaboration on cyber issues between agencies and departments. DOD is responsible for the defense of its networks, while DHS has primary operational responsibility for the defense of all Federal, unclassified civilian networks. Domestic cyber-attack and cyber-crime investigations are the responsibility of the FBI. There is certainly work to be done to fully operationalize these concepts and enhance cybersecurity collaboration within the government so that there is a broader unity of effort within government that helps to grow and enhance our nation's security posture.

In contrast, cybersecurity responsibilities within the private sector are far more diffuse. The security of each network is the responsibility of its owner or operator, meaning that the security of the vast majority of the country's cyber infrastructure is in the hands of hundreds of thousands of different entities. Coordination and information sharing between these entities is often limited, though significant progress has been made in some sectors through the growth of Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). In this diffuse environment, it is critical that the United States government assist the private sector in their cybersecurity efforts and work diligently to help facilitate critical cybersecurity information sharing, both among private sector actors and between the government and the private sector.

What makes information sharing so important is the fact that our cyber infrastructure is so diffuse. While one entity, such as the FBI, Google, or Microsoft, may be aware of a particular vulnerability or threat, it can take days, weeks, or even months before the relevant information spreads throughout the cyber ecosystem and results in the deployment of patches, installation of new technologies, changes in network architecture, or the adoption of new policies that adequately counter the threat. We have, admittedly, made significant progress in cyber threat information sharing over the past decade. I applaud the efforts of organizations such as the Financial Sector ISAC (FS-ISAC), the Multi-State ISAC (MS-ISAC), and the hundreds of other ISACs and ISAOs that have helped us get to where we are today—but the reality is that we can do more.

On the government side, we already have programs in place that provide the private sector with threat information data and other forms of assistance designed to help private organizations enhance their cybersecurity posture. These programs have had their successes, but it remains too difficult for those in the private sector to gain access to the wealth of information and assistance that the government, particularly DHS, could provide.

For example, DHS's National Protection and Programs Directorate (NPPD) operates the Cyber Information Sharing and Collaboration Program (CISCP), which can be an invaluable source of threat information data for private entities, potentially providing them with access to government threat information data, including sensitive, classified information. However, navigating the process to participate in this program and gain access to classified information can be daunting for private companies. To join the program, the company must first be aware of its existence, and in my experience too few companies are aware of CISCP and other assistance programs offered by

DHS and other government agencies. Once a company is aware of the program, it must then negotiate a Cooperative Research and Development Agreement (CRADA) with DHS, a type of agreement that was not originally designed to facilitate this type of information sharing. The negotiation of a CRADA, while relatively straight forward, can be confusing to companies unfamiliar with government processes or cooperative agreements and can take months to negotiate.

Further, even with a CRADA in place, a company will only have access to less sensitive types of government threat data—classified information remains off limits for a variety of reasons. The data companies do have access can also be incomplete, missing additional, unclassified threat information from agencies outside of DHS, such as the FBI, meaning that a company may need to receive threat information from multiple government entities to receive a more complete picture. To review more sensitive, classified threat information the private company will need to obtain the proper clearances for several of the company's representatives.

Fortunately, DHS can sponsor at least some company personnel for a clearance when a CRADA is in place, but here too are obstacles. The process for obtaining a clearance can be confusing and time consuming, especially for those in the private sector with no previous experience in national security or government service. Further, the Federal government continues to face a significant clearance process backlog. Last month, the Government Accountability Office released a report that found that the Office of Personnel Management's National Background Investigation Bureau currently has a backlog 710,000 background investigation cases, meaning that the entire clearance process can take upwards of a year.[9] Under these circumstances one can understand why a private company might choose to forgo access to more sensitive threat information.

In addition to process improvements, there are ways in which the government can make the threat information data they are already sharing more useful to the private sector. First, threat information sharing is significantly more efficient when it is automated, relying on standardized feeds and formats to communicate key pieces of data. DHS and the government writ-large should continue to encourage the automated sharing of threat information and push for greater interoperability between such initiatives, including the incorporation of confidence levels in the sharing of cyber threat indicators (such as IP addresses and MD5 hashes).

Second, the government should prioritize the identification and sharing of Tactics, Techniques, and Procedures (TTPs) as well as exploit targets for sharing with the private sector. Such information is increasingly important as cyber adversaries rapidly vary traditional signatures used to counter cyber-attacks, such as IP addresses and MD5 hashes. A greater understanding of the TTPs and exploit targets used by an adversary can allow security professionals to focus network hardening and detection efforts to more surgically address risks relevant to their environment, allowing them to prioritize internal controls and policies to match likely threat actor TTPs.

Third, the government should encourage further work on the development of a common language for the exchange of threat information—threat information data is most valuable when all of the organizations involved use the same terminology to describe various TTPs. Within the cyber field there is a significant focus on the Structured Threat Information eXpression (STIX) framework, however many practitioners leverage different frameworks (VERIS, for example) to manage threat TTP and incident information. I would recommend working to resolve the difference between the these various systems with a focus on defining a common language for sharing.

Fourth, the government should foster the collection and categorization of incident data to identify TTPs and other relevant information. A key source of TTP information lies in information collected as part of an incident response

[9] *See* https://www.gao.gov/assets/700/690499.pdf

effort. Thus, there needs to be a greater focus on “reverse engineering” incidents to identify TTPs utilized and corresponding courses of action that could mitigate such TTPs. DHS is currently sponsoring a Cyber Incident & Data Analysis Repository (CIDAR) initiative to define the architecture for an incident repository, however the success of such an initiative will come down to the willingness of organizations to contribute this data. As such, we must do all that we can to encourage companies, in addition to Federal government entities, to share this information in the name of enhancing our collective cybersecurity posture.

To that end, the government should also consider expanding the scope of the Support for Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act to include cybersecurity-related technologies in addition to anti-terrorism technologies. The SAFETY Act, first passed as part of the Homeland Security Act of 2002, provides incentives for the development and deployment of anti-terrorism technologies by creating systems of risk and litigation management. The act provides some terrorism-related liability limitations for organizations that adopt DHS-certified anti-terrorism technologies, creating an incentive for companies to invest and deploy these technologies. Expanding the safety act to include cybersecurity technologies would create a similar incentive for their development and adoption, ultimately encouraging an enhanced cybersecurity posture across the private sector. Legislation to expand the scope of the scope of the SAFETY Act, the Cyber SAFETY ACT of 2018, was recently introduced in the Senate by Senator Steve Daines (R-Montana).

Finally, the private sector has benefited greatly from the National Institute of Standards and Technology’s (NIST’s) Cybersecurity Framework. This voluntary framework, which consists of standards, guidelines, and best practices for organizations to manage cybersecurity-related risk, has been well received in both the private and public sectors. It has helped organizations prioritize and identify areas deserving of additional investment and attention while promoting the protection and resilience of cyber infrastructure across sectors. That said, NIST can continue to refine and enhance the framework as it continues to iterate and update the document. I would encourage NIST to focus on providing more specific, control-related guidance, providing industry with a clearer understanding of what actions organizations should be taking to implement a control. Such guidance would be in addition to providing references to other cybersecurity frameworks and control regimes as the current framework does.

Cyber Deterrence

The second area of cyber policy and strategy that I would focus on is cyber deterrence. While having the proper policies and technologies in place to defend our cyber infrastructure is important, it is equally important that we have the right tools at our disposal to successfully deter or respond to cyber adversaries from undertaking a cyber-attack in the first place. While we will never be able to deter every cyber-attack, we can use those that do take place to make it clear what responses we have at our disposal and indicate what costs we can inflict on those who undertake such an attack.

The most important question to address when contemplating cyber deterrence is that of attribution. While others testifying before this body are far more qualified to speak to the technical questions of attribution, the broader point remains—attribution of a cyber-attack to a specific actor is vital to providing the United States with the opportunity to use the full range of deterrent options at its disposal. Unfortunately, in the cyber realm attribution can be exceedingly difficult. Attackers can be adept at obfuscating their origins, will leverage tools, vulnerabilities, and TTPs pioneered by others, and leverage the systems of other unsuspecting victims to support and launch their attacks.

We have, fortunately, made significant progress on attribution, though many of the methods and technologies underpinning these capabilities remain highly sensitive. But even our advanced capabilities have limitations—

rarely does a cyber-attack have the sort of indisputable evidence that we have come to expect in the physical world. There may not be a smoking gun or a bloody knife. There won't be a satellite image of our adversary launching their cyber weapon at the United States and rarely is a cyber weapon system something that is exclusive to a single actor. Sometimes the evidence will ultimately come from signals or human intelligence rather than a forensic analysis of the attack itself. The reality is that much of the evidence available to us in the cyber realm is circumstantial, and the confidence level of an attribution can be just as important as the attribution itself.

While not ideal, this is a circumstance that we will ultimately have to come to terms with. We must continue to make investments in our capabilities but will need to rely upon the judgement of our intelligence agencies and technical experts. We may not have the time, or the ability, to wait for complete certainty. We may instead need to identify what level of confidence is needed in what circumstance.

Similarly, we need to ensure that we have a full range of options at our disposal when we respond to a cyber-attack to properly deter future attacks. Like in the physical world, those responses must ultimately be calibrated to the severity of the attack and specifics of the circumstance. As a result, the range of potential responses will range from diplomatic warnings to a proportional cyber response, from a criminal indictment to a kinetic strike on a physical battlefield. We must be prepared to leverage all our options and be certain to properly calibrate their severity to that of the cyber-attack. We must also make it clear that we are willing to use all the options at our disposal.

The criminal indictments obtained by Special Counsel Mueller for 13 Russian nationals and 3 Russian entities are examples of how we can leverage the criminal justice system.[10] The Department of the Treasury's recent targeted sanctions against various Russian national and entities, including 7 Russian oligarchs, similarly demonstrates how we can leverage targeted sanctions.[11] Broader sanctions, including economic and banking sanctions, can also be leveraged as both a response to a cyber-attack and a deterrent against future attacks. Offensive cyber activities and even kinetic military strikes may also be justified in certain circumstances. What is important is that the United States responds in a proportional manner and in one that deters our adversaries from taking similar action in the future.

We must also consider new ways in which we can cooperate and coordinate with our allies on cybersecurity, not just in terms sharing intelligence and capabilities, but in deterrence as well. Toomas Hendrik Ilves, the former President of Estonia and Visiting Fellow at the Hoover Institution at Stanford University, recently proposed what he termed a new "Cyber NATO," a coalition of liberal democracies that is better able to meet the ubiquity of cyber threats and ensure proper, adequate response.[12] The President of Microsoft, Brad Smith, has proposed what he has dubbed a "Digital Geneva Convention," which outlines the rules of cyberspace and protects civilians and other bystanders from the offensive cyber activities of nation-states.[13] These are the sorts of bigger ideas that we must also consider as the volume of cyber-attacks grows and our capabilities mature.

Conclusion

The size and scope of state-sponsored threats facing the US may seem daunting and it is important for us to recognize that we are unable to prevent all attacks. But altering our cyber defense and deterrence strategies will

[10] *See* https://www.justice.gov/file/1035477/download

[11] *See* https://home.treasury.gov/news/press-releases/sm0312 and https://home.treasury.gov/news/press-releases/sm0338

[12] *See* https://berlinpolicyjournal.com/a-digital-defense-alliance/

[13] *See* https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

go a long way toward mitigating the risk. Congress must act to address the shortcomings of the current security clearance process, consider expanding the scope of the SAFETY Act to include cybersecurity-related technologies to incentivize private sector companies to create innovative defense technologies, and simplify and standardize information sharing between the private and public sectors to ensure that it is easier for enterprises to share and receive threat information from the government in real time. Thank you to the Committee Chairman for inviting me to testify today. This hearing is a positive step in helping our country better defend against and deter cyber-attacks.