PERRY
WORLD
HOUSE
UNIVERSITY of PENNSYLVANIA

World House Student Fellows 2016-2017

Prevention in the Cyber Domain

By Itai Barsade, Louis Davis, Kathryn Dura, Rodrigo Ornelas, and Ariel Smith

Prevention in the Cyber Domain

Introduction

One of the most important trends in international politics over the last generation is the development and growth of cyber capabilities. Cyber activities advance a number of state and non-state actor objectives -- such as tactical military advantage, industrial espionage, infrastructure damage, espionage, and political interference. As the pre-eminent global power, the United States is both a propagator and largest victim of these activities. This makes understanding policy options in the cyber domain a critical topic both for the United States and for the globe.

Numerous scholars have attempted to investigate the recent development of cyber activities in the international sphere. To understand its implications, some researchers have focused on how cyber actions are similar to other weapons, to determine the best practices for containing and regulating them. For example, many draw comparisons between cyber and nuclear weapons, subsequent deterrence principles, and international agreements.[1] Other scholars investigate what norms, laws, and policies apply to the cyber world.[2] In fact, there is a consensus that the legal and political paradigms prescribing actions and reactions after cyber activities occur are either limited or non-existent.[3] Despite the lack of an overarching framework, researchers like Paul Meyer suggest that methods of prevention used by state and civil actors can be applied to cyber activities.[4]

[1] Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (2011): 18. http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-05_Issue-4/Nye.pdf.

Robert Litwak and Meg King, "Arms Control in Cyberspace?" *Wilson Center* (2015). https://www.wilsoncenter.org/sites/default/files/arms_control_in_cyberspace.pdf.

Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011). http://www.inss.org.il/uploadimages/Import/(FILE)1308129610.pdf.

Stephen J. Cimbala, "Cyber War and Deterrence Stability: Post-START Nuclear Arms Control," *Comparative Strategy* 33, no. 3 (2014). http://dx.doi.org/10.1080/01495933.2014.926727.

Martin C. Libicki. "Cyberdeterrence and Cyberwar." *RAND Corporation* (2009). http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[2] Catherine Lotrionte, "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence," *Georgetown Journal of International Affairs* (2013):75-88. http://www.jstor.org/stable/43134324.

Catherine Lotrionte, "Cyber Operations: Conflict Under International Law," *Georgetown Journal of International Affairs* (2012): 15-24. http://www.jstor.org/stable/43134334.

Mary Ellen O'Connell, "Cyber Security Without Cyber War," *Journal of Conflict & Security Law* 17, no. 2 (2012): 187–209.

[3] Pool, Phillip. "War of the Cyber World: The Law of Cyber Warfare." *The International Lawyer* 47, no. 2 (2013): 299-323. http://www.jstor.org/stable/43923953.

[4] Paul Meyer, "Cyber-Security through Arms Control: An Approach to International Co-operation," *The RUSI Journal* 156 no. 2 (2011): 22-27.

Most research, however, largely deals with cyber activities on a theoretical level dealing specifically with international agreements, law, and norms. Previous academic efforts to clarify cyber activities lack a degree of practicality necessary for policymakers. For example, most of the current literature fails to propose concrete recommendations for how to prevent a range of cyber activities. There is also the question of what constitutes cyber activities in the first place. The term 'cyber activities' itself is a broad term that, for the purposes of this paper, will entail any actions performed in the digital realm with the intention of disrupting a system or action, such as hacking into military, industrial, infrastructure, and governmental systems. Given this expansive definition, we create clarity from many different sources to identify potential policy recommendations aimed at preventing cyber activities in a variety of domains.

To fill the gap between academic research and the policy world, this policy paper develops and employs a five-stage model of cyber activities, using the insights derived from the model to explain key risks and possibilities in the cyber domain. The framework defines the various stages of hostile cyber activity, from its inception up to its perceived conclusion. The five stages are: prevention, in which we examine how to prevent and guard against hostile cyber attacks; preemption, in which we discuss what to do if adversaries are known to be planning such an attack; halting, in which we look at how to stop an ongoing attack; mitigation, in which we look at how to lessen and deal with the effects of an attack; and retaliation, in which we examine punitive measures taken after an attack.

Our target-specific recommendations differ based on the key players and variables involved in each situation, but we have identified a common thread in these recommendations. Overall, we propose that the United States government will have to take proactive action in order to prevent hostile cyber attacks. This may come in the form of baseline requirements for security standards on government-owned technological devices; it may also take the form of regulations in the private sector to mandate basic preventative practices. We recognize that the capabilities of cyber present a pressing national security issue and, in order to be adequately equipped to deal with their use by foreign actors, we recommend that the United States government take appropriate action to prepare itself for offensive cyber attacks..

In what follows, we outline the framework with illustrations of each stage and then delve into recommendations for the first stage, prevention. Within this stage, we examine key targets of cyber activities, including military, industrial, infrastructure, and governmental systems, and propose specific measures of preventing their disruption. While issues of attribution are inherent in the cyber field, our recommendations equally address both state and non-state actors since the goal is for all cyber-related disruptions to be prevented and limited. Similarly, cyber activities blur the lines of categorization; for example, some case studies, like the hack of Georgia's critical infrastructure in conjunction with a military front, are discussed in the specific context of one key target but could equally be placed into multiple. As a result, we then turn to an overarching summary of our recommendations in light of the categories' overlaps, and conclude.

A Five-Stage Framework for Understanding Cyber Activities

Background

This section presents a model that can be used to understand the general, end-to-end timeline of the most prevalent types of hostile cyber activity. Recognizing the evolution and fundamental characteristics of attacks throughout their entire duration can aid policymakers and relevant organizations to respond efficiently and design plans of action to coordinate defense measures. To illustrate the progression of an attack along the delineated stages, we include a brief case study of the 2014 Sony Pictures hack by listing its most important events within the stages to which they correspond under this model. We will focus on three main actors: Sony Corporation, the United States government, and the North Korean state.

This cyber-attack was attributed to North Korean hackers with the goal of preventing the release of the satirical movie *The Interview*, which mocked North Korean supreme leader Kim Jong-un and depicted his assassination.[5]

1. Prevention

At this first stage, the goal is to avert cyber activities from taking place by strengthening cyber defenses or minimizing the risks of hostile attacks. Mechanisms to achieve this purpose involve controlling and limiting the access of potential adversaries to equipment, specialized technical expertise, and computational resources that can be used to launch damaging cyber-attacks. This stage also encompasses a wide range of precautionary safety measures, such as imposing strict computer security regulations to manufacturers of hardware and software or conducting drills to find and repair vulnerabilities in existing systems. International agreements and treaties also fall within this category.

In the Sony case study, the United States conducted a number of preventive activities against North Korea in recent years. For example, worried about the growing threat of North Korean cyber and military resources, the NSA successfully infiltrated North Korean networks in 2010 and installed malware that allowed the US to spy on cyber activity.[6]

[5] "US attributes cyberattack on Sony to North Korea - The Washington Post." Accessed April 16, 2017. https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html.

[6] "N.S.A. Breached North Korean Networks Before Sony Attack, Officials ...." Accessed April 16, 2017. https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

2. Preemption

This stage is reached when prevention is unsuccessful. The main assumption is that there exists strong evidence that an attack is imminent, since the adversary has successfully obtained the necessary resources to launch it and has plans to do so. Thus, the principal focus of responders is impeding such an attack from taking place through the use of deterrent strategies ranging from diplomacy, to threats, and even preemptive strikes.

In June of 2014, North Korean foreign ministry officials publicly called the movie *The Interview* "an act of terrorism and war" and threatened to retaliate "merciless[ly]" if the movie were released.[7] While the United States initially did not officially conduct preemptive measures, it was revealed that Sony senior executives decided to remove some of the film's most controversial content in response to the threats[8].

3. Halting

This stage focuses on ongoing attacks that could not be preempted and have successfully managed to cause harm to systems or infrastructure. A fast response is critical, and efforts should concentrate on stopping and controlling the attack as soon as possible. This is most commonly done using defensive technical tools in order to identify attackers and prevent them from accessing vulnerable systems, or to restrict all network communications to prevent the hackers from obtaining sensitive information. Due to the heterogeneity of information systems and potential attacks, there exists a wide range of halting strategies. These should be defined and tested proactively so that they can be commenced as soon as the initial signs of an attack are detected.

In November of 2014, Sony was hacked by a group called "Guardians of Peace", which stole an estimated 100 terabytes of data—including sensitive information such as unreleased movies and scripts, private emails from senior executives, and personal information about employees. The attacks crippled Sony's networks, equipment, and communications, quickly thwarting all potential attempts to secure the compromised systems.[9]

[7] "North Korea threatens war on US over Kim Jong-un movie - BBC News." Accessed April 16, 2017. http://www.bbc.com/news/world-asia-28014069.

[8] "The Interview: film at center of shocking Sony data ... - The Guardian." Accessed April 16, 2017. https://www.theguardian.com/film/2014/dec/12/the-interview-sony-data-hack.

[9] "Sony Pictures hack appears to be linked to North Korea, investigators ...." Accessed April 16, 2017. https://www.washingtonpost.com/world/national-security/hack-at-sony-pictures-appears-linked-to-north-korea/2014/12/03/6c3c7e3e-7b25-11e4-b821-503cc7efed9e_story.html.

4. Mitigation

At this point in the timeline, the attackers have been at least partially controlled and the primary attacks have stopped, so the focus shifts to minimizing the damage of the attacks on the integrity of systems, infrastructure, and privacy. Through strategic partnerships, responders assess the critical risks and focus on finding the optimal solutions to avoid further detrimental effects.

After the initial cyber attacks on Sony in November of 2014, the hacker group made public threats about attacking US cinemas that showed *The Interview.* Additionally, they threatened to keep leaking sensitive information unless Sony would promise to never release the movie in any form.[10] Sony responded by canceling the movie's release to prevent further leaks since the company was suffering from substantial damage to its public image as a result of controversial sensitive information that the hackers published.[11] President Obama publicly disagreed with Sony's decision, due to its implication that a foreign government was effectively enforcing censorship in the United States.[12] Sony later reversed this decision, and decided to release the movie through online streaming services.[13]

5. Retaliation

This stage usually takes place after the previous four have been overcome, and it encompasses punitive measures that explicitly respond to particular attacks in order to establish strong disincentives for future attackers. Retaliation mechanisms include the use of economic sanctions, political sanctions through international organizations, and the launch of retaliatory cyber or kinetic counterattacks if the magnitude of the original attack warrants them. Due to the unique characteristics of cyber warfare, responders should be aware of the uncertainties in attribution and risks of escalation when deciding plans of action.

After the Sony cyber-attacks, North Korea suffered from a widespread internet outage, which its government publicly attributed to the United States.[14] On the other

[10] "Hackers to Sony: We'll stand down if you never release ... - CNN Money." Accessed April 16, 2017. http://money.cnn.com/2014/12/19/media/insde-sony-hack-interview/.

[11] "Sony emails reveal Jennifer Lawrence paid less than ... - The Guardian." Accessed April 16, 2017. https://www.theguardian.com/film/2014/dec/12/sony-email-hack-jennifer-lawrence-paid-less-american-hustle.

[12] "Hackers to Sony: We'll stand down if you never release ... - CNN Money." Accessed April 16, 2017. http://money.cnn.com/2014/12/19/media/insde-sony-hack-interview/.

[13] "Sony Releases 'The Interview' Online - WSJ." Accessed April 16, 2017. http://www.wsj.com/articles/sony-to-release-the-interview-online-christmas-eve-afternoon-1419442648.

[14] "North Korea blames US for Internet outages, calls Obama ... - Reuters." Accessed April 16, 2017. http://www.reuters.com/article/us-northkorea-cybersecurity-idUSKBN0K502920141228.

> hand, the White House publicly attributed the Sony hacking to the North Korean nation state, and President Obama published an executive order that targeted North Korean organizations and government officials with economic sanctions as a response to the cyber attacks. [15]

While in practice all the different stages are interrelated, and the progression of cyber attacks may seem more continuous than discrete, this framework is useful to pair the main events in the chronology of any attack with the most appropriate responders and plans of action. This paper will now focus on the first of our stages - prevention - and examine the four most important categories of cyber activity that we identified: military warfare, industrial espionage, threats to critical infrastructure, and attacks on governmental systems. The following sections will explore each category within the context of United States policy-making, present case studies of relevant historical precedents, and propose recommendations to strengthen preventive and defensive capabilities in both the private and public sectors.

Military Use

Introduction

In order to understand prevention of cyber attacks in the military domain, it is also necessary to understand the broader context of military applications of cyber activities as a means of advancing tactical and strategic objectives held by a nation. As such, this section will first layout the military applications of cyber activities, delineate typical stakeholders, and overview the broad objectives of employing cyber activities in the military sphere. With this background information in mind, this section will then discuss a case study of how cyber activities were used to advance military objectives in the Ukrainian conflict. Finally, with a firm grasp of the purpose of cyber activities in the military domain and an example of how they were used, this section will develop a series of recommendations for policymakers to consider in order to support prevention-oriented policies.

Key Takeaways

- Military applications of cyberspace operations can serve three functions: offensive operations used to project power through force, defensive operations used to protect the various elements of friendly cyberspace, and information network operations used to design, build, and run military networks.
- Cyber activities can serve as a means of asymmetric warfare against a militarily superior force

[15] "Timeline: North Korea and the Sony Pictures hack - USA Today." Accessed April 16, 2017. https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.

- Russia’s use of malware to target Ukrainian artillery units is an example of how cyber activities can advance tactical and strategic military objectives -- thus, providing a benchmark for policymakers considering prevention-oriented policies.
- To avoid the cyber vulnerabilities on the battlefield, policymakers should consider measures that limit soldier interactions with public platforms that undermine operational security.
- To combat cyber attacks on the battlefield and integrate cyber capabilities into traditional operations, the military must embed cyber operators in combat units during training exercises.
- To support prevention of hostile cyber activities, policy makers must increase manpower in cyber-oriented units through competing with private sector salaries and creating special Reserve-duty opportunities.

Background

As warfare continues to evolve, cyber activities take on several purposes. According to the Army Field Manual on Cyber and Electromagnetic Activities (FM 3-38), cyberspace operations “are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”[16] More specifically, cyberspace operations can be divided into three functions. The first function is offensive cyberspace operations (OCO), which are “conducted to project power by the application of force against enemies and adversaries in and through cyberspace. More specifically, offensive operations can be used to achieve multiple objectives, such as: destroying enemy equipment and forces, disrupting networks and communications, degrading the quality of enemy sensors, and deceiving the enemy to believe false realities about the battlespace. The second function is defensive cyberspace operations (DCO), which are operations “conducted to defend DOD or other friendly cyberspace and preserve the ability to utilize friendly cyberspace capabilities.” Finally, Department of Defense information network operations are meant to “design, build, configure, secure, operate, maintain, and sustain networks.”[17] Core to these operations is the notion that cyberspace is a crucial element of any modern-day military; and as such, it must be used both defensively and offensively to achieve tactical and strategic goals.

As the United States continues to adapt new cyber capabilities, its adversaries are employing cyberspace operations to advance their tactical and strategic objectives. Given the United States’ military superiority, the development of cyber capabilities will pose a source of asymmetric power for adversaries. To better understand the application of cyber operations by adversaries, the next section will discuss the Russian use of malware to achieve tactical victories against Ukrainian artillery units found in Eastern Ukraine.

[16] Department of the Army. 2014. "FM 3-38." Field Manual , Washington D.C.

[17] Ibid.

Case Study: Ukrainian Artillery Hack

In December 2016, Crowdstrike – a threat-intelligence firm – released a report on reported Russian hacking of Ukrainian artillery units. In the report, Crowdstrike claims Russia implanted a malware program within an Android application developed for use by Ukrainian artillery officers. The malware is called "XAgent," and is used by an organization associated with Russian Military Intelligence (GRU) – "FANCY BEAR." FANCY BEAR, which is one of the organizations responsible for the 2016 DNC Election Hack, uses XAgent to collect and transmit data from Android operating system and Apple iOS.[18]

Per Crowdstrike, the original software intended to make Ukrainian artillery forces more efficient when using their D-30 howitzers. However, FANCY BEAR's implant of malware into the software resulted in the transmission of location data back to Russian forces. In turn, "the successful deployment of this application may have facilitated reconnaissance against Ukrainian troops." [19] In turn, Crowdstrike alleges that this malware is connected to Ukraine's loss of 15%-20% of their pre-war D-30 arsenal.[20] Moreover, this application is only one example of Russia's broader use of cyber activities to achieve success in the conflict in Ukraine. More specifically, various sources allege that Russia has shut down Ukrainian military systems and targeted soldiers using cellphones (Foreign Policy, 2014), (Breaking Defense, 2015).[21][22] If true, this employment of offensive operations represents one of the first times that cyberspace was incorporated fully into a military's pursuit of achieving tactical and strategic objectives.

Current practices and recommendations

Since recognizing cyberspace as a part of the general battlespace, the United States formed Cyber Command to address gaps and build capabilities in cyber activities and warfighting. The purpose of cyber command is to integrate the chain of command, work with allies, and marshal all resources towards supporting OCOs, DCOs, and information network operations.[23] While this represents progress, there are a number of key recommendations that will both prevent hostile cyber attacks and improve military capabilities more broadly.

[18] NJ Cybersecurity. 2016. *X-Agent.* https://www.cyber.nj.gov/threat-profiles/trojan-variants/x-agent.

[19] Crowdstrike. 2016. *Danger Close: Use of FANCY BEAR Android Malware in Tracking of Ukrainian Field Artillery Units.*

[20] It is important to note that the original report (December 2016) released by Crowdstrike alleged these numbers closer to 80%. However, Crowdstrike revised these estimates (March 2017) following analysis by International Institute for Strategic Studies.

[21] Reuters. 2016. *Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'.* December.

[22] Foreign Policy. 2014. *Hack Attack.* March.

[23] Lynn, William J. 2010. "Defending a New Domain." *Foreign Affairs.* https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

A key challenge for the military is the effective integration of cyber forces into front-line combat operations. To address this, Cyber Command's National Mission Force is adding "two network defense specialists" to the staff of every brigade – with the purpose of augmenting the number of experts on the battlefield who can target enemy systems.[24] In addition to this offensive tasking, the National Mission Force is also responsible for protecting Defense Department networks. Despite these changes, there still exists a significant cultural gap between Cyber and tactical combat units.[25] As such, we recommend that the military continue to integrate cyber operators in combat training operations. By training with cyber operators, combat units will learn to effectively marshal the full range of resources and capabilities available to them to advance battlefield objects. This will support both offensive and defensive priorities. That is, the mission for cyber operators is not solely to disrupt, degrade, deceive, and destroy the adversaries systems. Rather, these cyber operators will also handle the front-line defense of crucial cyber systems that support combat systems and logistics. Regarding prevention, this move will enable the military to protect themselves against already proven adversary operations – such as the Russian hack of Ukrainian artillery software.

Another key challenge facing the military is the procurement of talent. Recently, Army Cyber Command established two pilot programs to facilitate the recruitment of civilians with cyber skills.[26] Without adequate manpower, the United States military and other organizations will be unable to effectively prevent cyber attacks. Given the competitiveness of the private sector, the United States government should attract talent by implementing benefits and rewards for individuals who have or commit to acquiring skills germane towards cyber activities. At the end of the day, the United States government will be unable to fully compete with the salaries and general quality of life afforded by the private sector. As such, recruitment strategies should also focus on facilitating special reserve programs that retain talent on a part-time basis.

Finally, keeping the preceding case study in mind, it is important that the military strive to keep soldiers separated from public systems that compromise operational security. In the Ukrainian case, soldiers were targeted as a result of two factors. First, they accessed a software for military use over a military forum on the internet. Second, they utilized that software on their cellphones while deployed to the frontline. By exhibiting basic cyber hygiene -- for example, not downloading software over unsecure lines and using one's cell phone during combat -- the military can avert potential hostile attacks.

[24] Freedberg, Sydney J. 2016. *Army Wargames Hone Battlefield Cyber Teams.* http://breakingdefense.com/2016/11/army-wargames-hone-battlefield-cyber-teams/.

[25] Freedberg, Sydney J. 2015. *Army Fights Culture Gap Between Cyber & Ops: 'Dolphin Speak'.* http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/.

[26] Federal News Radio. 2017. *Army Cyber flies two pilots to bring in cyber recruits.* http://federalnewsradio.com/defense/2017/02/army-cyber-looks-new-ways-bring-recruits/.

Industrial espionage

Introduction

This section will examine the threat that state and non-state actors' cyber activities pose for United States private enterprise through industrial espionage. First, this section will contextualize the threat of industrial espionage. Second, this section will examine a prominent case study of industrial espionage executed by China, which is the most prolific nation currently conducting such attacks. Last, it will cover the scant current practices in place to deal with industrial espionage, and will propose recommendations on how to best prevent this type of hostile cyber activity.

Key Takeaways

- Industrial espionage represents the infiltration of foreign governments, hackers, or companies into private American companies, and the subsequent theft of sensitive private information or intellectual property from those companies.
- The theft of this private information can lead to larger consequences such as issues with arms control, the safety of economic information, and unfair trade deals.
- To standardize cyber security, the United States government must take positive action to establish basic technological security standards within private businesses.

Background

Industrial espionage poses even more of an existential threat than ever as the capabilities of technology allow small hacking groups to pose as major actors working for the aims of foreign governments. This section will investigate a current case of industrial espionage and pose recommendations for the United States government when dealing with such cases.

In the case of prevention, industrial espionage refers to the infiltration of foreign governments, hackers, or companies into private American companies, and the subsequent theft of sensitive private information or intellectual property from those companies. Chinese and Russian hackers currently represent the most prominent threat to United States Targets.[27]

This is dangerous for a myriad of reasons. Hackers can obtain information on technologies that took years, or decades, to develop; they can receive insider information on United States business strategy, or even a jump on negotiations.

There are also cases of industrial espionage that do not seem to take aim at our nation itself, rather, at individuals for profit. In 2015, the Department of Justice cited how "organized, multinational criminal enterprises have arisen to steal large volumes of credit card numbers and other personally identifiable information."[28] These criminal enterprises then sell the stolen

[27] Office of the National Counterintelligence Executive. "Foreign Spies Stealing US Economic Secrets in Cyberspace." *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011. https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[28] "Criminalizing the Overseas Sale of Stolen U.S. Financial Information." The United States Department of Justice. March 20, 2015. Accessed April 16, 2017. https://www.justice.gov/archives/opa/blog/criminalizing-overseas-sale-stolen-us-financial-information.

personal information to the highest bidder. While this is damaging and can cause many problems for American individuals and the breached companies, it does not typically signify malicious intent by a foreign actor or government and as such further discussion of it will be withheld from these recommendations.

Case Study: Sun Kailing hack

Consider, in 2014, when the United States government charged Chinese government officials with orchestrating cyber espionage; it was "the first time the U.S. [had] formally charged foreign government officials for explicitly acting at the behest of a foreign government in cyber crimes."[29] The charges, brought by a federal grand jury in Pennsylvania, listed the targeted companies as Alcoa World Alumina, Westinghouse Electric Co. (a nuclear power developer), Allegheny Technologies, U.S. Steel Corp., United Steelworkers Union, and SolarWorld (a solar technology company).

"In some cases, they stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen," Attorney General Eric Holder said. "In others, they stole sensitive, internal communications that would provide a competitor, or adversary in litigation, with insight into the strategy and vulnerabilities of the American entity. In sum, the alleged hacking appears to have been conducted for no reason other than to advantage state-owned companies and other interests in China, at the expense of businesses here in the United States." The Chinese government denied these allegations.

Along with trade secrets, this industrial espionage has other implications. It can largely be seen as intelligence-gathering for Chinese state-owned industry to gain a competitive advantage on American corporations or a jump ahead on technological developments. At the time of the hack, Westinghouse was in the process of negotiating a deal with a Chinese state-owned company; and stolen emails included information on the American company's plans for these negotiations.[30] Also stolen from Westinghouse by hacker Sun Kailing of the PRC (listed by the FBI as one of its "most wanted"[31] were "design specifications on pipes, pipe supports and pipe routing, enabling Chinese competitors to build world-class nuclear power plant without doing the research themselves."[32]

[29] Massimo Calabresi. "US Charges Chinese Government Officials With Cyber Crimes." Time. May 19, 2014. Accessed April 16, 2017. http://time.com/104508/u-s-charges-chinese-government-officials-with-cyber-espionage/.

[30] Sam Frizell. "What Did Chinese Hackers Actually Steal From US Companies?" Time. 2014. Accessed April 16, 2017. http://time.com/106319/heres-what-chinese-hackers-actually-stole-from-u-s-companies/.

[31] "SUN KAILIANG." FBI Most Wanted. May 19, 2014. Accessed April 16, 2017. https://www.fbi.gov/wanted/cyber/sun-kailiang.

[32] Frizell, *What Did Chinese Hackers Actually Steal*.

A challenge here is how to manage and respond to these events. In the event of attacks on private companies, those companies are allowed to act at their own discretion and are not beheld to the United States government to behave in any particular way. Often, companies don't even know their data has been stolen.

Current practices and recommendations

We do not recommend that corporations make an effort to retaliate on their own terms, when they suspect foreign involvement, without first involving the United States government.

That being said, the meeting between Obama and Xi Jinping in 2015 stands as an almost singular precedent when dealing with foreign cyber hacks. In this meeting they both pledged that their governments would "refrain from computer-enabled theft of intellectual property for commercial gain,"[33] and Obama maintained the possibility of sanctions if Chinese hacks were to continue. A second vague promise followed that both leaders would seek "international rules of the road for appropriate conduct in cyberspace," for which we can refer to the literature review.[34]

Finally, we recommend basic government-mandated security practices and measures taken to prevent such cyber hacks, for example, two-factor authentication on any device that includes company information. These rules currently do not exist and leave corporations vulnerable to a theft of information.

Critical Infrastructure

Introduction

This section will delve into the threat that state and non-state actors' cyber activities pose for critical infrastructure (CI), another crucial sector vulnerable to cyber actions. First, it will provide background information on the definition of critical infrastructure and on which major players are involved in defending against potential cyber activity. Second, to illustrate instances where cyber actions hindered a country's critical infrastructure, the section will discuss two case studies: the Russian government and/or non-state actors attacking Estonia and Georgia. Last, it will discuss current practices and propose policy recommendations for both public and private entities for how to best prevent CI disruptions from cyber adversaries in light of current practices.

Key Takeaways

- Critical infrastructure is defined to be vital physical or virtual systems in sectors such as commercial, communication, energy, and transportation whose disruption would be detrimental to American society and national security.

[33] Julie H. Davis and David E. Sanger. "Obama and Xi Jinping of China Agree to Steps on Cybertheft." September 25, 2015. Obama and Xi Jinping of China Agree to Steps on Cybertheft.

[34] Ibid.

- Alleged Russian DDoS, disruption and denial of services, attacks in Estonia and Georgia are examples of cyber activities succeeding in disrupting large-scale critical infrastructure function.
- To minimize security vulnerabilities, rigorous, standardized measures are necessary for every critical infrastructure actor, public and private.
- To create a national baseline of cyber security, all critical infrastructure actors must develop active communication and integration.
- To maintain standardized prevention measures, government actors below the federal level, including state and local-level, involved with protection must be empowered through increased resources.

Background

According to the United States Department of Homeland Security, the term 'critical infrastructure' includes "assets, systems, and networks, whether physical or virtual…so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[35] This definition encompasses commercial, communication, energy, transportation, and other sectors which bridge both public and private control. As such, maintaining critical infrastructure security must involve all major players including "Federal, state, local, tribal, and territorial (SLTT) entities… public and private owners and operators"[36] and international partners. The Department of Homeland Security oversees and directs the federal effort to protect the nation's CI. In other words, the Secretary of Homeland Security identifies and prioritizes CI, heads the coordination efforts of other key departments, agencies, and actors, conducts vulnerability assessments, coordinates federal responses to incidents involving CI, aids in CI investigations, reports its findings, etc.[37] Meanwhile other departments, such as Department of State, Department of Justice Department of the Interior, and the Intelligence Community, also play significant roles by focusing on their areas of expertise and engaging private and international partners in the process.

Given that our proposal focuses on cyber activities, this section will deal solely with threats to CI derived from cyber means alone. Therefore, some threats include, but are not limited to, "infiltration of a network from the outside; exfiltration, disclosure, exposure, or corruption of stored data, or rendering stored data inaccessible…local or widespread disruption of services," etc.[38] One common form of cyber-attack is DDoS or disruption and denial of

[35] "Critical Infrastructure Sectors," *U.S. Department of Homeland Security*, December 30, 2016, https://www.dhs.gov/critical-infrastructure-sectors.

[36] "Presidential Policy Directive --Critical Infrastructure Security and Resilience," *President Barack Obama White House Archives*, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[37] Ibid.

[38] "The National Plan for Research and Development in Support of Critical Infrastructure Protection," *U.S. Department of Homeland Security* and *Office of Science and Technology Policy*, 2004, https://www.dhs.gov/xlibrary/assets/ST_2004_NCIP_RD_PlanFINALApr05.pdf, 29.

services. This method overwhelms a cyber system by "forcibly inserting tasks, dramatically increasing demands on a system, or denying availability of needed resources such as communication systems."[39] Such actions render cyber infrastructure vulnerable and ultimately inoperable for the people who need them.

Case Studies: Russian Cyber Activities in Estonia and Georgia

From April to May 2007, Estonia was subject to cyber activities. The country had decided to relocate a "Russian World War II memorial and Russian soldier's graves."[40] In return, hackers, using botnets and DDoS methods, temporarily disabled the nation's Internet which greatly hindered Estonia's ability to function. Botnets are "hijacked computers" that generate the masses of information used in DDoS attacks.[41] Since the botnets can be installed well in advance, the computer user may not even be aware that their device is participating in the cyber activities. Additionally, the DDoS attack disrupted their communications by targeting government offices, news organizations, and financial institutions.[42] Thus, Estonia's banks were forced to limit their operations and move to proxy servers in Lithuania. Additionally, Estonia cut abroad access to its sites to curb foreign influence.[43] For a small country dependent on the Internet and foreign trade, these attacks were hugely detrimental in the short-term.

The Russian government denied any involvement despite numerous international accusations to the contrary. Russia had plausible deniability since most electronic "fingerprints" originated from ordinary computers around the world including within Estonia itself.[44] Given the use of botnets, this is unsurprisingly. Also, due to the hackers using fake internet protocol (IP) addresses, there was no conclusive evidence for who was responsible.[45] In December 2011, a member of a pro-Kremlin youth movement, Konstantin Goloskokov, "admitted that he and some of his associates launched the 2007 attacks on Estonia."[46]

[39] Ibid., 34.

[40] Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News*, December 18, 2016, http://www.nbcnews.com/news/us-news/timeline-ten-years-russian-cyber-attacks-other-nations-n697111?cid=public-rss_20161218.

[41] Major William C. Ashmore, *Impact of Alleged Russian Cyber Attacks* (Fort Leavenworth, Kansas: School of Advanced Military Studies US Army Command and General Staff College, 2009): 7.

[42] Dr. Andrew Foxall, "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain," *Russia Studies Centre at the Henry Jackson Society*, no. 9 (2016): 5-6.

[43] "A cyber-riot; Estonia and Russia," *The Economist* 383, no. 8528 (2007): 55.

[44] Ibid.

[45] Ashmore, 6-7.

[46] Foxall, 6.

In 2008, Georgia faced an onslaught of DDoS attacks after the government sent troops into South Ossetia, a republic backed by Moscow.[47] Russia responded militarily, and seemingly, coordinated the physical attack with a complementary cyber front. Two to three weeks before the physical war broke out, Georgia's cyber infrastructure was assaulted. Its governmental, communication, transportation, and finance networks were hindered such that citizens were unable to access web sites for information.[48] Ultimately, an Internet blockade was enacted.[49] During a time of such heightened tensions and subsequent war, effectively shutting down the Internet and communications across the country had enormous implications not only for daily Georgian life and the conflict itself but for the future of war more generally.

Much like the Estonian incident, Russian officials denied involvement in the attack. However, it seems highly implausible that the coordinated fronts were simply a coincidence. Experts suggest that the Georgian attack was the work of a "St. Petersburg-based criminal gang, known as the Russian Business Network, or RBN."[50] However, given that pro-Russian websites posted instructions for how to conduct such attacks and provided the necessary software, seemingly anyone could have contributed to the attack.

Current practices and recommendations:

In 2004, the Department of Homeland Security released a national plan to protect CI. In this proposal, the government sought to achieve broad, strategic goals such as "Inherently Secure Next-Generation Computing and Communication Network: Devising threat mitigation and countermeasures for proactive protection" and "Resilient, Self-Diagnosing, Self-Healing Physical and Cyber Infrastructure Systems: Develop shielding and sacrificial systems to enhance protection and maximize resilience."[51] To attain these goals, the plan emphasized the role of research and development to explore new means of protection and collaboration with intelligence communities and local law enforcement to receive warning of impending attacks and respond efficiently. The 2013 Presidential Policy Directive for Critical Infrastructure Security and Resilience echoes these sentiments of integrating all major players into protecting CI, including public CI owners and operators.[52]

The 2004 national plan puts forward three recommendations for security. First, it emphasizes "ensuring that protective identification, confirmation, and authorization access

[47] Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations."

[48] John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 12, 2008, accessed April 5, 2017, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[49] David J. Smith, "Russian Cyber Strategy and the War Against Georgia," *Atlantic Council*, January 17, 2014, http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.

[50] Foxall, 5.

[51] "The National Plan for Research and Development in Support of Critical Infrastructure Protection," 28.

[52] "Presidential Policy Directive --Critical Infrastructure Security and Resilience."

measures are rigorous and well managed."[53] Second, it recommends "providing redundancy, re-routing options, and self-healing or self-sustaining attributes to rapidly restore or at least provide a minimum level of service until recovery actions can be implemented for both cyber and physical systems."[54] Third, it endorses "having procedures in place to minimize shifting of vulnerability by diverting detection systems, security and law enforcement personnel, and response teams to less optimal configurations, thus leaving certain locations less well protected."[55] In other words, the government should create and maintain rigorous authorization measures, develop means to restore or at least maintain minimal function even during an attack, and limit resource diversion given that it could result in new vulnerabilities.

Our recommendations build on the existing prescriptions. We, too, find the need for rigorous authorization measures to be imperative for prevention. An agreed-upon baseline of general measures should be consistent for all actors involved in CI, from private to public. As a result, we propose the creation of a close working relationship between every CI actor to develop, maintain, and frequently reassess these standards. While the 2013 Presidential Policy Directive for Critical Infrastructure Security and Resilience touches on this cooperation, it fails to recommend a national baseline of security. Finally, the local government actors involved with CI protection must be empowered to contribute to the prevention. The term 'public actors' in policy documents typically refers to the federal government players as opposed to the state or local-level officials who can be more influential to the private CI owners. However, this local level often lacks access to the same, necessary prevention resources as the federal government. Creating uniform policies across all actors requires more resources going to those overlooked in the process, the local public officials.

Government-to-government (G2G) attacks

Introduction

This section will be dedicated towards exploring the threat of government-to-government cyberattacks. In contrast with military attacks, industrial espionage, and critical infrastructure attacks, this mode of cyberwarfare is focused exclusively on attacks conducted by the government of one state actor (perpetrator state) on another government (victim state). These public sector attacks are waged through formal federal government departments, agencies, or ministries, usually an entity within the perpetrator state's intelligence community.

Key Takeaways

- Government-to-government cyber attacks pose a credible threat to the national security apparatus of all nations and the personal information of civil servants
- Russia's attack on the DNC demonstrates the need for adherence to the strictest form of preventative measures and guidelines to deter future provocations

[53] "The National Plan for Research and Development in Support of Critical Infrastructure Protection," 34.

[54] Ibid.

[55] Ibid.

- Political parties should mirror the cybersecurity practices of governmental agencies and departments given the sensitive nature of the information collected and retained through local, state, and national election periods

Background

The objective for the perpetrator state in a government attack varies depending on the specific example, but is most typically related to the extraction/theft of one of two types of sensitive information from the victim state: Personally Identifiable Information (PII) and national security documents of the victim state for which a prior level of security clearance is warranted for viewing. PII is defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[56] This includes, but is not limited to, home addresses, personal phone numbers, credit card information, and financial history of current and past government employees. A third type of sensitive information extracted during a government attack is a broad category to encompass any and all information, even if not officially deemed non-classified in nature, from a government entity.

Specifically within the United States government (USG), there are three levels of security clearance; from lowest to highest, they are Confidential, Secret, and Top-Secret. These security clearances are required to view USG documents related to national security matters, and are granted to USG employees only after an intense and length background check process. Other states in the international system have a similar classification system and background check process required for the viewing of classified public sector information; hence, when a perpetrator state extracts such information, it does so to gain access to internal government-specific documents not meant for unauthorized sharing with the general public, allies, and adversaries unless they formally are declared to be declassified.

By examining recent a recent example, one can better understand the mechanics behind government-to-government attacks. In particular, the Russian government cyberattack on the United States government in summer 2015 and spring 2016 will be explored; through this attack the Russian government collected internal documents of the Democratic National Committee (DNC), the governing body for the United States' Democratic Party, in the lead up to the 2016 U.S. Presidential Election. Exploring the case study on the Russian hack of the DNC will enable one to solidify ways to expand upon current preventive practices in place to deter and block subsequent attacks.

[56] General Services Administration, "Rules and Policies - Protecting PII - Privacy Act," https://www.gsa.gov/portal/content/104256. See OMB M-10-23 (Guidance for Agency Use of Third-Party Website and Applications) for original coining of PII definition.

Case Study: Russian Hack of the Democratic National Convention (DNC)

During the summer of 2016, the Russian Government waged a cyber-attack against the Democratic National Convention, gaining access to thousands of emails and attachments related to party activity in the lead up to the U.S. Presidential Election between Donald Trump and Hillary Clinton. These documents were then shared with DCLeaks.com and WikiLeaks as well as Guccifer 2.0. On October 7, 2016, a joint statement authored by the Department and Homeland Security and the Office of the Director of National Intelligence concluded that "based on the scope and sensitivity of these efforts, that only Russia's senior-most [government] officials could have authorized these activities."[57] A subsequent Joint Analysis Report (JAR) on the cyberattack was published by the Department of Homeland Security (DH) and Federal Bureau of Investigation (FBI) in December 29, 2016 to provide more technical details on the mechanisms used by the Russian civilian and military intelligence services (RIS) to compromise networks related to the U.S. election and government.[58]

Current practices and recommendations:

Some of the more immediate practices that should be adopted by government entities to prevent future government cyberattacks are succinctly listed in the 2016 DHS-FBI report. These include maintaining backups of critical information training staff in best practices, updating applications that are particularly vulnerable to attacks, segmenting networks into "logical enclaves," and the setting up firewalls to block data from specific IP locations or applications.[59] The DNC cyberattack highlights the need for the same stringent rules for cyberwarfare prevention to apply not only to official federal departments, agencies, and ministries, but also quasi-governmental entities such as political party organizations. This will enable federal governments to ensure a cohesive approach to countering subsequent attacks.

Conclusion and Summary of Recommendations

Within a world today that is dependent on information systems, governments are faced with the unique challenge of how to best counter cyber activities in a number of domains. Using our five-stage model consisting of prevention, preemption, halting, mitigation, and retaliation, we have discussed how the United States government can best prevent and respond to risks and possibilities in the cyber domain. For the several cyber activities discussed, including military warfare, industrial espionage, threats to critical infrastructure, and attacks on governmental systems, prevention arguably serves as the most immediate area of focus for public and private actors alike. These major players can and should proactively implement sound policies to deter future enemy cyber actions and mitigate their potential damage. In sum, we recommend that policymakers:

[57] DHS and ODNI, "Department of Homeland Security and Office of the Director of National Intelligence on Election Security." October 7, 2016.

[58] NCCIC and FBI. "GRIZZLY STEPPE – Russian Malicious Cyber Activity." December 29, 2016.

[59] Ibid.

- To avoid the cyber vulnerabilities on the battlefield, policymakers should consider measures that limit soldier interactions with public platforms that undermine operational security.
- To combat cyber attacks on the battlefield and integrate cyber capabilities into traditional operations, the military must embed cyber operators in combat units during training exercises.
- To support prevention of hostile cyber activities, policy makers must increase manpower in cyber-oriented units through competing with private sector salaries and creating special Reserve-duty opportunities.
- Continue to establish bilateral memorandums of understanding specifically related to cybersecurity, focusing on actionable and clear reforms
- Mandate uniform and robust government cybersecurity practices to prevent cyber disruptions
- Integrate local and federal public stakeholders with private actors to establish a common baseline for preventative measures
- Hold political parties (quasi-governmental entities) to the same cybersecurity standards as government entities such as departments and agencies.

Works Cited

“A cyber-riot; Estonia and Russia.” *The Economist* 383, no. 8528 (2007): 55.

Ashmore, Major William C. *Impact of Alleged Russian Cyber Attacks*. Fort Leavenworth, Kansas: School of Advanced Military Studies US Army Command and General Staff College, 2009.

Calabresi, Massimo. "US Charges Chinese Government Officials With Cyber Crimes." Time. May 19, 2014. Accessed April 16, 2017. http://time.com/104508/u-s-charges-chinese-government-officials-with-cyber-espionage/.

Cimbala, Stephen J. “Cyber War and Deterrence Stability: Post-START Nuclear Arms Control.” *Comparative Strategy* 33, no. 3 (2014): 279-286. http://dx.doi.org/10.1080/01495933.2014.926727.

“Critical Infrastructure Sectors.” *U.S. Department of Homeland Security*. December 30, 2016. https://www.dhs.gov/critical-infrastructure-sectors.

"Criminalizing the Overseas Sale of Stolen U.S. Financial Information." The United States Department of Justice. March 20, 2015. Accessed April 16, 2017.

https://www.justice.gov/archives/opa/blog/criminalizing-overseas-sale-stolen-us-financial-information.

Crowdstrike. 2016. *Danger Close: Use of FANCY BEAR Android Malware in Tracking of Ukrainian Field Artillery Units.*

Davis, Julie H., and David E. Sanger. "Obama and Xi Jinping of China Agree to Steps on Cybertheft." September 25, 2015. Obama and Xi Jinping of China Agree to Steps on Cybertheft.

Department of the Army. 2014. "FM 3-38." Field Manual , Washington D.C.

DHS and ODNI. "Department of Homeland Security and Office of the Director of National Intelligence on Election Security." October 7, 2016.

Federal News Radio. 2017. *Army Cyber flies two pilots to bring in cyber recruits.* http://federalnewsradio.com/defense/2017/02/army-cyber-looks-new-ways-bring-recruits/.

Foreign Policy. 2014. *Hack Attack.* March.

Foxall, Dr. Andrew. "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain." *Russia Studies Centre at the Henry Jackson Society*, no. 9 (2016).

Freedberg, Sydney J. 2015. *Army Fights Culture Gap Between Cyber & Ops: 'Dolphin Speak'.* http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/.

—. 2016. *Army Wargames Hone Battlefield Cyber Teams.* http://breakingdefense.com/2016/11/army-wargames-hone-battlefield-cyber-teams/.

Frizell, Sam. "What Did Chinese Hackers Actually Steal From US Companies?" Time. 2014. Accessed April 16, 2017. http://time.com/106319/heres-what-chinese-hackers-actually-stole-from-u-s-companies/.

General Services Administration. "Rules and Policies - Protecting PII - Privacy Act." https://www.gsa.gov/portal/content/104256.

Libicki, Martin C. "Cyberdeterrence and Cyberwar." *RAND Corporation* (2009). http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Litwak, Robert and Meg King. "Arms Control in Cyberspace?" *Wilson Center* (2015). https://www.wilsoncenter.org/sites/default/files/arms_control_in_cyberspace.pdf.

Lotrionte, Catherine. "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence." *Georgetown Journal of International Affairs* (2013): 75-88. http://www.jstor.org/stable/43134324.

Lotrionte, Catherine. "Cyber Operations: Conflict Under International Law," *Georgetown Journal of International Affairs* (2012): 15-24. http://www.jstor.org/stable/43134334.

Lynn, William J. 2010. "Defending a New Domain." *Foreign Affairs.* https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Markoff, John. "Before the Gunfire, Cyberattacks." *The New York Times*. August 12, 2008. Accessed April 5, 2017. http://www.nytimes.com/2008/08/13/technology/13cyber.html.

Meyer, Paul. "Cyber-Security through Arms Control: An Approach to International Co-operation." *The RUSI Journal* 156, no. 2 (2011): 22-27.

NCCIC and FBI. "GRIZZLY STEPPE – Russian Malicious Cyber Activity." December 29, 2016.

NJ Cybersecurity. 2016. *X-Agent. https://www.cyber.nj.gov/threat-profiles/trojan-variants/x-agent*

Nye Jr., Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (2011): 18-38. http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-05_Issue-4/Nye.pdf.

Office of the National Counterintelligence Executive. "Foreign Spies Stealing US Economic Secrets in Cyberspace." *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011. https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

O'Connell, Mary Ellen. "Cyber Security Without Cyber War." *Journal of Conflict & Security Law* 17, no. 2 (2012): 187–209.

Pool, Phillip. "War of the Cyber World: The Law of Cyber Warfare." *The International Lawyer* 47, no. 2 (2013): 299-323. http://www.jstor.org/stable/43923953.

"Presidential Policy Directive --Critical Infrastructure Security and Resilience." *President Barack Obama White House Archives*. February 12, 2013.

https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Reuters. 2016. *Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'.* December.

Smith, David J. “Russian Cyber Strategy and the War Against Georgia.” *Atlantic Council*. January 17, 2014. http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.

"SUN KAILIANG." FBI Most Wanted. May 19, 2014. Accessed April 16, 2017. https://www.fbi.gov/wanted/cyber/sun-kailiang.

Tabansky, Lior. “Basic Concepts in Cyber Warfare,” *Military and Strategic Affairs* 3, no. 1 (2011): 75-92. http://www.inss.org.il/uploadimages/Import/(FILE)1308129610.pdf.

“The National Plan for Research and Development in Support of Critical Infrastructure Protection.” *U.S. Department of Homeland Security* and *Office of Science and Technology Policy*. 2004. https://www.dhs.gov/xlibrary/assets/ST_2004_NCIP_RD_PlanFINALApr05.pdf.

Windrem, Robert. “Timeline: Ten Years of Russian Cyber Attacks on Other Nations.” *NBC News*. December 18, 2016. http://www.nbcnews.com/news/us-news/timeline-ten-years-russian-cyber-attacks-other-nations-n697111?cid=public-rss_20161218.