Diana Hallisey

POL4700-A

Professor Russell

15 May 2020

A Comprehensive Cybersecurity Policy for the United States Government According to Cyberattacks and Exploits in the 21st Century

Introduction

Adversaries launch cyberattacks or cyber-exploits with contrasting intentions and desired outcomes. A cyberattack is a malicious attempt by a state, third party, or individual to disrupt a computer's network; whereas, a cyber-exploit is an action that uncovers and steals "confidential" information from a computer's data. [1] Within this research paper, the main adversary of such cyberattacks and/or exploits will be the nation-state. The victims of these cyberattacks will range from multinational corporations, such as Sony, to nuclear programs in Iran. This essay will focus on four motivations behind such cyberattacks: (1) private sector hacking (the theft of intellectual property) (2) political gains (3) infrastructure destruction (4) military power. This paper will examine the following cyberattacks: Sony Pictures Hack, Equifax, meddling of the 2016 Presidential Election, OPM Hack, 2015 Ukraine Power Grid Attack, Stuxnet, and Russo-Georgian Cyberattacks. The cyberattacks will serve as a basis to draft a comprehensive United States Foreign Policy that addresses each of the four incentives within a broader cybersecurity strategy. This paper will first explain the diversity of such attacks. Following the analysis, the paper will seek to answer

[1] Susan Landau, "Listening In: Cybersecurity in an Insecure Age" (Yale University Press, 2017), page 50.

this pressing question: *What should the implementation of United States Foreign Policy look like according to contrasting, yet substantial cyberattacks in the past?*

Cyberattacks

Private Sector Hacking

The Sony Pictures Hack of 2014 was the epitome of a destructive cyberattack on the private sector, but it also represents the difficulty of attribution within cyberspace. This cyberattack entailed the deletion of Sony's hard drive and the theft of confidential information. The attackers, which have been referred to as the "Guardians of Peace", destroyed Sony's startup software and revealed private details about producers, actors, and other employees by the use of "spear phishing", which is not a very sophisticated attack. The federal government of the United States has since stated that intelligence has consistently linked the hack with the North Korean government, yet it has repeatedly denied such an attack. [2] The cyberattack escalated into coercion; the hackers threatened Sony to stop the screening of *The Interview*, a movie that includes the assassination of Kim Jong Un. The Sony Pictures Hack demonstrates a very real threat of cyberattacks to corporations, yet this could have been mitigated with stricter security notions. Unfortunately, Sony was quite susceptible to this cyberattack because the company only depended upon human-made passwords, which skilled hackers can easily guess. The Sony Pictures Hack of 2014 shows the significance of multifactor authentication (MFA) within a secure system. Sony lacked MFA, which NIST defines as a "*security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account*". [3] Sony now understands the

[2] Andrea Peterson, "The Sony Pictures hack, explained", *The Washington Post*, 2014.

[3] NIST, "Back to basics: Multi-factor authentication (MFA)", *US Department of Commerce*.

importance of stronger cybersecurity measures within its systems; therefore, adversaries will have a more difficult time infiltrating the company's networks.

Equifax is one of the large credit reporting agencies within the United States. The Equifax Breach of 2017 was another example of state-sponsored hacking on the private sector. After years of investigation, the Department of Justice stated that the People's Liberation Army of China was to blame for the cyber-exploit. The company's website acquired a vulnerability that has since been coined CVE-2017-5638 on its web portal. [4] This vulnerability allowed adversaries to execute malicious code in its HTTP. The attackers then obtained access to Equifax's other servers due to weaknesses within its system. The Equifax Breach of 2017 was unprecedented regarding the type of information revealed and the amount of people it affected. The cyber-exploit was the perfect storm, and Fruhlinger explains the devastation of such theft. He states, "*It potentially affected 143 million people — more than 40 percent of the population of the United States — whose names, addresses, dates of birth, Social Security numbers, and drivers' licenses numbers were exposed"*. [5] This exploitation was launched in conjunction with the Office of Personnel Management (OPM) hack and Marriott's 2018 attack. The purpose of these attacks was to learn more about United States' government officials and operatives. [6] The United States' private sector is a massive target to external actors, such as China, and the private sector acts as a gateway for information; therefore, its cybersecurity measures are exceedingly important to the federal government. The collaboration between the private and public sectors are necessary in order to establish a secure and comprehensive approach to national and international cybersecurity policies.

---

[4] Joshua Fruhlinger, "Equifax data breach FAQ", *CSO*, 2020.
[5] Ibid.
[6] Ibid.

Political Gains

The Office of Personnel Management (OPM) Hack occurred in 2015. The OPM Hack has been one of the most intrusive data breaches against the US government throughout the 21st century. There has been minimal, concrete evidence to suggest that China launched the cyber-exploit, yet there is growing consensus that the OPM hack was a part of several state-sponsored attacks to steal sensitive US governmental data. The hackers obtained access to SF-86 forms, as well as clearance adjudication information. The SF-86 is a required form for national security positions, and it comprises of sensitive information, such as an individual's social security number, place of residence, and family members. The information needed for a clearance adjudication far exceeds that of a SF-68, which is very concerning for the 21.5 million government employees who fell victim to the hack. [7] The OPM cyber-exploit is a classic example of cyber-espionage, and it also demonstrates the need for a robust cybersecurity strategy within United States Foreign Policy. This hack drove President Obama and President Xi Jingping to negotiate a bilateral agreement in cyberspace called the US-China Cyber Agreement of 2015, which specifically focused on the theft of intellectual property.

The meddling of the 2016 Presidential Election was the quintessence of how influential outside nations can be within US domestic politics. The Senate confirmed that Russia was indeed the culprit behind the cyber-meddling in April of 2020. Russia exerted its cyber-capabilities by "*engaging in cyber-espionage and distributing messages through Russian-controlled propaganda outlets to undermine public faith in the democratic process, hurting Democratic candidate Hillary Clinton and helping President Donald Trump*". [8] The Russian government targeted former

[7] Michael Adams, "Why the OPM Hack is Far Worse Than You Can Imagine", *Lawfare*, 2016.
[8] Aljazeera, "Senate panel confirms Russian interference in 2016 US election", *United States News*, 2020.

Democratic candidate Hillary Clinton. The hackers utilized "spear phishing" to access John Podesta's emails, who was Clinton's campaign chairman. He changed his password with the corrupted link, which allowed the group to continue and maximize their phishing efforts within the campaign. The group then gained access to the Democratic National Committees' computers and posted their findings on a separate website. In addition to these hackings, Russia influenced Americans through social media platforms. The New York Times reports, "*Russian agents intending to sow discord among American citizens disseminated inflammatory posts that reached 126 million users on Facebook, published more than 131,000 messages on Twitter and uploaded over 1,000 videos to Google's YouTube service*". [9] This cyberattack clearly had political motivations, and it is a solemn warning for cybersecurity measures towards free and fair elections within liberal democracies. Russia further polarized the United States, which has been evident since the election of President Donald Trump in 2016.

Critical Infrastructure

Stuxnet was one example of how cyberspace can impact critical infrastructure. Critical infrastructure is "*the underlying components of the economy that run our modern-day civilization, ranging from power and water, to banking healthcare, and transportation*". [10] Stuxnet is an intricate worm that the United States and Israel created and used on an Iranian nuclear facility (Natanz) in order to stall the development of its nuclear weapons. Stuxnet is exceedingly sophisticated – the mobility and speed of the worm was unprecedented when it was discovered in 2010. Stuxnet particularly targets uranium centrifuges, in which the worm alters the machines' programming. The modification in the code hastens the production process, which tarnishes the

[9] Michael Isaac, "Russian Influence Reached 126 Million on Facebook Alone", *The New York Times*, 2017.
[10] Alison Russell, "Cybersecurity: Key Terms and Acronyms", *Cybersecurity: Directed Study*, 2020.

equipment in the process. [11] Kruhlinger continues, "*...while this is happening, the PLCs tell the controller computer that everything is working fine, making it difficult to diagnose what's going wrong until it's too late*". [12] The worm damages the system, yet those who are monitoring the system cannot detect any problems within the software, which demonstrates the complexity and success of Stuxnet. In retaliation to these cyberattacks, Iran launched a series of hacks on the United States' financial sector. Iranian cyber-capabilities have enhanced exponentially since the discovery of Stuxnet, which conveys that the United States must think about ways in which it will advance its defenses. The manifestation of physical destruction illustrates how damaging technological attacks can be on a nation-state, and many groups have utilized the worm to attack other forms of infrastructure, such as gas lines and water pumps.

The 2015 Ukraine Power Grid Cyberattack also represents how attacks can degrade and destroy critical infrastructure within a country, which undeniably harms individual and national security. This was the first cyberattack that effectively and uniquely disrupted a power grid, which is a network center for providing electricity to consumers. The attack closely mirrored the beginning of Sony and Clinton's campaign. Within this usage of "spear phishing", the adversaries delivered emails with faulty Microsoft attachments, and unfortunately, the users opened these documents, which granted system access to the hackers. The crucial difference is that the design of this attack was distinctly created for the Ukrainian power grid, which made the recovery from such an attack more difficult. Landau states, "*Hackers disconnected at least twenty-seven substations, shutting off power to about 225 million customers for one to six hours*".[13] The cyberattack also disabled generators. Landau asserts that the cyberattack was preventable through

[11] Joshua Fruhlinger, "What is Stuxnet, who created it and how does it work?", *CSO*, 2017.
[12] Ibid.
[13] Landau, Page 21.

multifactor authentication (MFA). Three employees did not use MFA at the distribution center, which made hacking the power grid that much easier. This case proves that robust defensive systems are necessary in order to protect critical infrastructure, will be incorporated within the broader cybersecurity plan.

Military Hybrid

South Ossetia has been a point of contention between Russia and Georgia since the collapse of the Soviet Union in 1991. The dispute over this region created ongoing struggles between both nations, which have since been transformed into a case study for "cyberwarfare". Russian-led cyberattacks on Georgia was a hybrid case that involved political gains and military power, and the conflict became a prime example on how nations can utilize cyberattacks as an effective part of their greater military strategy. The Russo-Georgian conflict highlighted an important theme: the changing dynamics of modern warfare, which now undeniably incorporates cyberspace. Specifically, Russia launched a series of DDoS attacks, which is defined as "*attacks where hackers distribute overwhelming traffic across multiple sources, often using botnets of thousands or even millions of machines*". [14] The attacks targeted government websites, which left the government

[14] Alison Russell, "Cybersecurity: Key Terms and Acronyms", *Cybersecurity: Directed Study*, 2020.

unable to use its broadcast transmitters, which incited widespread panic across Georgia. Many civilians feared a Russian invasion. The Russian hackers successfully disabled Georgian servers. The New York Times reports that the website of former Georgian president Mikheil Saakashvili was inoperable for approximately 24 hours. [15] These chaos attempts by Russia has not halted at the Russo-Georgian War – chaos has become a popular objective within their cyberattacks.

Cyberspace Initiatives & Agreements

The US-China Cyber Agreement of 2015 is a bilateral agreement that was negotiated between President Obama and President Xi Jingping. The agreement addresses cyber relations between both countries. The most crucial principles that were set forth by the presidents are as follows: the prohibition of supporting or conducting cyber-related theft of intellectual property, establishment of high-level dialogue on fighting cybercrime, further discussions to identify and foster global norms in cyberspace, and the agreement to respond to malicious cyber activity within a timely manner. [16] The policy does engender important precedents for cyber relations, such as open dialogue and bilateral (mutual) understandings in cyberspace, yet it does not sufficiently resolve the tensions between both countries. Cyber-espionage continues to plague the United States' private and public sectors.

Government Group of Experts (GGE) is a subdivision within the United Nations that discusses cybersecurity as a crucial component of global peace and security. As of 2020, there are twenty-five members, which includes three of the most active countries within cyberspace (United States, China, Russia). The Government Group of Experts convene four times throughout the year

[15] John Markoff, "Before the Gunfire, Cyberattacks", *New York Times*, 2008.
[16] CRS Insight, "US-China Cyber Agreement", 2015.

for about one week at a time. [17] A majority of the twenty-five members agree that pre-existing international law applies to cyberspace, yet unfortunately, the members fail to address the clash between global principles and national agendas; therefore, there are a multitude of questions that have not been answered by the GGE.

The United States and Western Europe have criticized the Russian-led United Nations Resolution regarding cybercrime. The European official stated, "*The big picture is that Russia and China are seeking to establish a set of global norms that support their view of how the internet and information should be controlled*". [18] Russia aspires to have more flexibility and control over its cyber-capabilities and operations. Putin has repeatedly asserted that the treaty set forth within the Budapest Convention of 2001 infringes upon national sovereignty. The Russian-led UN Resolution seeks to replace this treaty by prioritizing national sovereignty over international efforts to combat cybercrime, yet this presents several issues. First, the lack of cohesion in cyberspace further complicates peaceful relations or future bilateral/multilateral agreements among countries. Second, the treaty would give more protections to cyber-criminals. Third, the absence of collaboration within cyberspace would maximize cyberattack and cyber-exploits.

Recommendations

Private Sector Hacking

The United States' private and public sectors must enhance communication and collaboration since the federal government heavily relies on its networks and systems. The United States is exceedingly vulnerable for four reasons: the country is dependent upon cyber-controlled

[17] Geneva Internet Platform, "UN GGE and OEWG", 2020.
[18] Ellen Nakashima, "US urging a no on Russian-led UN resolution calling for a global cybercrime treaty", *Stars and Stripes*, 2019.

systems, private companies own and operate national systems, there is a lack of regulation when it comes to these private corporations, the US military is net-centric, which makes them extremely susceptible to attack. [19] According to the United States Accountability Office, the private sector expects the public sector to provide timely and crucial cyber-threat information, yet federal partners do not reliably report such threats. On the other hand, the public sector stakeholders expect the private sector to execute and implement their distinct plans, yet the private sector does not always strictly listen to such guidelines. The Sony Pictures Hack and the Equifax Breach both show the vulnerabilities within the private sector; therefore, greater regulation and exchange between both entities could truly minimize the theft of intellectual property. For example, the government could encourage the usage of multifactor authentication (MFA) throughout private sector networks and systems.

Political Protections

The meddling of the 2016 Presidential Election is a warning against cyberattacks for the 2020 Presidential Election, yet the Trump Administration and the Republican-controlled Senate have failed to address this impending threat. This failure to act is a direct danger to election security and the notion of democracy. The American public, as well as political parties, should be informed upon disinformation and cyberattacks, yet this can only occur if the federal government provides the resources and tools necessary to parties, the media, and citizens. Countries, such as France and Germany, have maximized their cybersecurity measures when it comes to foreign interference within elections. The French government provides cybersecurity seminars in order to minimize the knowledge gap between technical experts, government officials, and policymakers; whereas the

[19] Richard Clarke, Cyber War: The Next Threat to National Security and What to Do About It, 2010.

German government developed a "hack-back" strategy. [20] The most crucial component is open dialogue between the government and its citizens, which is seriously lacking within the United States.

The OPM Hack of 2015 inspired the US-China Cyber Agreement, yet this bilateral agreement has several shortcomings, which can be mitigated if the provisions below are included.

The provisions will extrapolate upon the "global norms" provision within the US-China Cyber Agreement. The policy will focus on developing, or constructing attitudes, guidelines, and international laws that shape the way in which nations view and regulate cyberspace. The first step would be educating policymakers and government officials on cybersecurity since there is a knowledge disparity among high-ranking members. Once education is provided domestically, policymakers will be able to create global standards and legal frameworks that will provide a basis for cyber-relations. [21] In addition to the existing policy's provisions, there will be a section where the U.S. and China establish a "cyber alliance". The cyber alliance entails the combination of diplomacy and cybersecurity specialists in order to communicate threats, responses, and cybercrime. The alliance would additionally bring sincerity to the agreement, and the interconnection of these fields would potentially lead to a more amicable and regulated cyberspace.

Critical Infrastructure

The 2015 Ukraine Power Grid Cyberattack and Stuxnet both represent how outside actors can impact vital state operations. The United States must protect its critical infrastructure with the most sophisticated and modern defenses. The private sector owns most of the cyber-reliant infrastructure; therefore, a strong relationship between the sectors are required in order to secure

[20] David Corn, "How to Stop Russia Attacking and Influencing the 2020 Election", *Mother Jones*, 2019.
[21] *For example, both nations can define the term "cybercrime" internationally, which will spread awareness and facilitate understandings in its detection, effects, and reactions.*

these systems. The United States heavily relies upon its infrastructure; therefore, resources and spending should be directed to its protection. The current administration is currently utilizing public key cryptography to secure operations, which is a step in the correct direction, yet the government should also establish strict guidelines that require companies to use multifactor authentication. The administration should also bridge the gap between both sectors by offering joint-cybersecurity seminars and workshops.

Military Strategy

The Russo-Georgia War demonstrates the evolution of warfare, in which cybersecurity has a fundamental role in offensive and defensive strategies. The United States must be aware of such tactics, yet the most important step the government can take towards its military strategy is to educate high-ranking military officials on cybersecurity measures. Additionally, it is important to have an interdisciplinary approach to this field; therefore, the communications among technical experts, computer scientists, cybersecurity policy analysts, cryptographers, and military officials are exceedingly important in national defenses.

Conclusion

In summation, a comprehensive, cybersecurity foreign policy must acknowledge, address, and incorporate each of the four motivations behind such cyberattacks. Private sector hacking, political gains, infrastructure destruction, and military power acquire different implications for the victims of such cyberattacks. The United States must learn from its own cyberattacks and cyber-exploits, as well as other attacks that have occurred across the globe in the 21st century. Understanding the vulnerabilities of other systems can help the United States establish a strong

offensive and defensive system that minimizes the effects of private sector hacking, cyber-meddling in elections, confiscation of personnel data, and infrastructure damage.

Works Cited

Adams, Michael. *Why the OPM Hack is Far Worse Than You Imagine*, Lawfare, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine, 2016.

Clarke, Richard. *Cyber War: The Next Threat to National Security and What to Do About It*, 2010.

Corn, David. *How to Stop Russia Attacking and Influencing the 2020 Election*, Mother Jones, https://www.motherjones.com/politics/2019/09/how-to-stop-russia-from-attacking-and-influencing-the-2020-election/, 2019.

CRS Insight, *US-China Cyber Agreement*, https://fas.org/sgp/crs/row/IN10376.pdf, 2015.

Fruhlinger, Joshua. *Equifax data breach FAQ*, *CSO*, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html 2020.

Geneva Internet Platform, *UN GGE and OEWG*, https://dig.watch/processes/un-gge#view-7541-5 2020.

Landau, Susan. *Listening In: Cybersecurity in an Insecure Age*, Yale University Press, 2017.

Markoff, John. *Before the Gunfire, Cyberattacks*, New York Times, https://www.nytimes.com/2008/08/13/technology/13cyber.html, 2008.

Nakashima, Ellen. *US urging a no on Russian-led UN resolution calling for a global cybercrime treaty*, Stars and Stripes, https://www.stripes.com/news/us/us-urging-a-no-vote-on-a-russian-led-un-resolution-calling-for-a-global-cybercrime-treaty-1.607671, 2019.

NIST, *Back to basics: Multi-factor authentication (MFA)*, US Department of Commerce,

https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication.

Peterson, Andrea. *The Sony Pictures hack, explained*, The Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/ 2014.

Russell, Alison. *Cybersecurity: Key Terms and Acronyms*, Cybersecurity: Directed Study, 2020.