The Harvard Undergraduate Foreign Policy Initiative

US CYBERCOM RUSSIA

Russian Cyber Capabilities and Vulnerabilities:

Analyzing the Cyberoperations of the Russian Government

Sama Kubba
Sim Sayer
Newaz Rahman
Syed Ahmed
Andrew Lu

FALL 2021

About the Authors

Newaz Aziz Rahman (newazrahman@college.harvard.edu) is an undergraduate at Harvard College pursuing a concentration in Government and a secondary in Economics. He is the policy chair for this project. He is interested in American foreign policy, international relations, global hegemons, and diplomacy.

Syed Umar Ahmed (sya437@g.harvard.edu) is an undergraduate student at Harvard Extension pursuing a concentration in Government and a minor in Computer Science. He is the senior director of operations for HUFPI and has worked for Apple and Amazon as a technical specialist and problem solver, respectively. He is experienced in market research, analysis and forecasting. He is also experienced in computer programming, and network security and is a CEH (Certified Ethical Hacker). His focus in this paper was on Russian Cyber Units and policy recommendations.

Andrew Lu (alu@college.harvard.edu) is an undergraduate at Harvard College with an intended concentration in Government and Statistics. He is the Deputy Director of Recruitment for HUFPI and is particularly interested in understanding the role of technology and the economy in modern policy-making and diplomacy. His experience centers on policy regarding technological innovation, economic development, and international relations. His focus in this paper was on case studies and policy recommendations.

HUFPI X USCYBERCOM
Russian Cyber Capabilities and Vulnerabilities

This document serves the purpose of providing an analysis of the cyberoperations of the Russian government.

Background

Since the creation of ARPANET and the subsequent variations of constructed networks, there have always been security flaws in the underlying structure of the Internet. These vulnerabilities are inherent in the switches, routers, and servers owned by Internet Service Providers and telecommunication carriers. With much of the Internet Protocols (IPs) having been engineered nearly 40 years ago to facilitate traffic through these networks, not much has changed in this IP system. This approach in creating the Internet has developed a space in which attackers and defenders take turns in exploiting and patching network vulnerabilities. Yet, attacks aren't the only cause for concern in this environment. Reliance on these networks has made it important to prevent malfunctions in the infrastructure that might impede the effectiveness of many of our government agencies. And as far as attacks are concerned, there are gaping holes in many of the different layers of the open systems interconnection (OSI) model, whether at the network, transport or application layer. The datalink layer, for example, has often been attacked through alteration of the manufacturer's code in switches, and flooding attacks can overwhelm switches and cause their malfunctioning. Similarly, switches that help aid the transfer of data packets to its destination can also be attacked and used to reroute traffic to an attacker's desired location. There are just a few methods out of a plethora of attack vectors that can and have been used.
The nature of the Internet Protocols during its creation was to promote the most cost-effective way to relay information across networks, but this has come at the cost of security. The same can be said for the Global Information Grid which has been maintained by the US Department of Defense. If any one layer in the OSI model is compromised, due to each layer's interdependency the next layer up in the model would not be aware and could pass compromised packets of data through the network towards its destination.

The systemic issue in creating sound cybersecurity measures is that these measures often need to evolve to defend against the emerging threat landscape. When software updates are pushed through enterprises and government systems, attackers begin to scope for security weaknesses in the new updates. And although there are many security monitoring software applications to aid in the detection of these attacks, they cannot defend against advanced persistent threats (APTs). With a dedicated enough attacker, especially those spooned by state governments such as Russia, their resources allow them to become persistent threats that wait for opportune moments to strike. Defending against this is one of the main challenges that government agencies and the private sector face. Another consideration of importance when discussing APTs is the motivation for attacks. Russia has been known for its hybrid warfare campaigns in Eastern Europe and

disinformation campaigns in the United States along with cyberattacks on critical infrastructure. This approach to cyber has characterized Russia as a malign actor that seeks to cause disruption and chaos in the states that it attacks. This differs from cyberattacks we've seen from China, which deal more with the theft of intellectual property and more economic centric attacks. The malign intention from Russia proves them to be the most formidable opponent in the cyber realm because they are the most malicious in their attacks and reasoning.

Cyberattacks have immensely damaging effects on the US economy due to a number of compounding factors. Cyberattacks can create effects across multiple organizations and sectors as the effects cause a ripple across the entire economy (Council of Economic Advisers 2018). The Colonial Pipeline cyberattack sharply decreased fuel supply lines, raising worries to businesses that utilize energy and consumers who needed gasoline. Another issue is that security vulnerabilities carry across different platforms and organizations, so cyberattacks may be able to successfully hit multiple targets. While the costs are difficult to quantify, the Council of Economic Advisors in 2018 estimated a roughly $57 to $109 billion cost as a result of such malicious activities. More than directly to business, cyberattacks can also target key infrastructure across the country (Allianz). Power generation, energy, transportation, telecommunications, and manufacturing are all areas where infrastructure is vulnerable to attack. The failure of one area of the infrastructure may lead to a chain reaction of technical failures. Cyberattacks target not only data but also control systems, making it difficult to recover any information or repel the attack. In particular, if cyberattacks successfully hinder federal agencies from performing their jobs, it may lead to a reduced ability to govern efficiently and effectively (CNN).

Currently, the United States appears to be primarily directing its efforts toward cybersecurity and less toward offensive actions. As such, a mix of cyber and tangible (e.g. economic) attacks for deterrence or retaliation may be appropriate at certain times. Just because Russia has strong cyber offensive capabilities does not necessarily mean that it also has a high level of security. Roughly 98% of surveyed Russian companies believed that their cybersecurity standards were not sufficient (Global Risks Insights, Morgan 2019). Further, because Russia has involved itself in so many offensive cyber attacks, it has become increasingly isolated in its preparation of cybersecurity. Take, for example, Russia's public declaration of alarm at the US' retaliatory cyber attacks. The fact that Russia takes to the media and does not just quietly address it means that it is either afraid or incapable to allow their cyber defense to speak for itself (Aljazeera 2021). Thus, collaboration with other governments and countries may yield stronger abilities for cyberattacks on different angles for effective action.

Analysis

The Russian government has maintained its adversarial status in the cyber realm since its first attack in 1996, the Moonlight Maze attack. With widely available documentation on their cyber strategy and with continued attacks that stem from the country, Russia has made an effort to publicly display its cyber prowess while at the same time denying their involvement. Many of the techniques that Russia used in the 1996 cyberattack on the U.S. are still used today. Avoiding detection by routing communications through third party servers, building backdoors to exfiltrate data over time, and sitting on vulnerabilities for extended periods of time (using APT techniques). And, with the advancement of technologies and procedures, the continued use of these techniques have become more sophisticated. When looking at the SolarWinds attack for example, we saw that Russian operatives accessed networks and systems from within the United States to avoid detection due to domestic surveillance laws. This indicates an evolving threat not only in technical capabilities but also in the understanding of rules and regulations to enhance attacks. In our analysis, we have taken into account past attacks, techniques used, and responses after the attack is discovered.

After performing a top down analysis of Russian cyber capabilities and vulnerabilities, we have found some key overlying trends that characterizes the operations and intent of the Russian government. We suspect the Russian government to continue its efforts in reducing network vulnerabilities due to their level of domestic surveillance and control of their network connections. We also suspect that Russian capabilities will increase in sophistication with the use of advanced AI in the scanning and detection of vulnerabilities in foreign networks, harder to detect disinformation campaigns, and continued advanced persistent threats (APTs).

Due to Russia's autocratic nature, much of the Russian internet is heavily surveilled by the Kremlin. This ability serves two purposes. On one end, it gives them greater insight on domestic dissidents and political movements. On the other, it allows the Kremlin to gain better insight on their networks and detect intrusions, making the role of offensive operations more difficult for CYBERCOM.

A particular trend that has stood out has been the use of widespread pirated software within Russia. The country has repeatedly appeared in the USTR Special 301 Report for the last few decades, meaning that intellectual property theft is highly prevalent in Russia. Although CYBERCOM cannot take advantage of this widespread use of pirated software, it can if the Russian government is using pirated software. During a policy inspection of Roskomnadzor (Federal Service for Supervision of Communications, Information Technology, and Mass Media), investigators found pirated versions of Microsoft, Adobe, Corel and Autodesk were found. Even pirated software from 1C, Russia's largest IT company, was found on Roskomnadzor's computers. If the watchdog that is responsible for supervising exploited IP and pirated software is using unreliable software, we assume that there are other agencies doing the

same. Although this was discovered in 2013, we have found that in 2021 Russia's Ministry of Education was reportedly using a counterfeit copy of Microsoft Word. In all, it is estimated that 62% of all software in Russia is pirated. If we can discover which government agencies are using them, we can use them as a target.
(Russia endured a lot of damage from NotPetya, even though they deployed it, because updated patches weren't able to be applied to pirated software).

The third trend that we see inhibiting our offensive operations is Russia's increasing ability to control their network access. With the recent developments of the Polar Express submarine cable, and an expected completion date of 2026, we suspect the Russian government to increase efforts in isolating the "RUnet". Although other means of data transmission are possible, with satellite and cellular tower infrastructure, the simultaneous efforts of establishing a new submarine cable and repeated tests for a "sovereign internet", by shutting down outside access into their networks, suggests that the Russian government is serious about isolating their networks. This further jeopardizes CYBERCOM's ability to use known network routes in the future.

The fourth trend that we see emerging, is Russia's continued exploitation of third party vendors and services to gain access into their desired targets. Due to the nature of U.S. infrastructure and economy, the majority of critical infrastructure is controlled by the private sector. This creates difficulties in America's ability to detect network intrusions and attacks. By using supply chain vulnerabilities in the development of software and by exploiting smaller segments of corporations, Russia has been able to advance its level of intrusion into larger networks, as was done with the SolarWinds attack.

Russian Cyber Units[1]

Military Intelligence - The Main Directorate of the General Staff (GRU)	High operational tempo. Control several research institutes that develop hacking tools and malware.
Unit 26165 (APT28)	Responsible for hacking the Democratic Congressional Campaign Committee, DNC, presidential campaign of Hilary Clinton. Operations against political, government, and private-sector targets in the US and Europe
Unit 74455 (Sandworm)	Responsible for the release of stolen emails and documents during the 2016 US presidential election. Unit 74455 appears to have significant offensive cyber capabilities. Responsible for the NotPetya Malware attack in 2017.
The Foreign Intelligence Service (SVR)	Operations have focused on collecting intelligence as opposed to causing damage. Known to have high levels of technical expertise.
APT29 (Cozy Bear)	Appear to focus on collecting intelligence and remaining undetected after it gains access to targeted networks. Reports have linked the SVR group to cyber espionage on COVID-19 vaccine research, tools of cybersecurity firm FireEye, and the SolarWinds attack.
The Federal Security Service (FSB)	Operations focus on protecting Russia from foreign cyber operations and monitoring domestic criminal hackers.
Berserk Bear, Energetic Bear, Gamaredon, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala.	FSB coerces civilian and criminal hackers to work as contractors with the threat of imprisonment. One FSB team focuses on penetrating infrastructure and energy sectors, focusing on reconnaissance or clandestine surveillance. Another group is capable of manufacturing its own advanced malware tools and is reported to manipulate its malware to mimic other hacking teams and conceal its activity.
The Federal Protective Service (FSO)	Responsible for the physical and electronic security of the government. Maintains the security of Russian government communications and is primarily concerned with the defense of government networks. No reports indicated offensive operations.
The Internet Research Agency (troll factory)	A private organization funded by Yevgeniy Prighozin, a close Putin confidant. Focuses on disinformation campaigns by impersonating domestic activists and people through social media. Responsible for efforts to sow discord and influence the US political system in 2016.

The FSB's continued operations in recruiting cyber criminals and coercing civilians for contracted cyber operations is indicative of a lack of qualified personnel within the government. We expect this lack of talent to persist in Russia's future operations, serving as a bottleneck in

[1] Bowen, Andrew S., and Library of Congress. Congressional Research Service issuing body. Russian Cyber Units. [Library of Congress public edition]., Congressional Research Service, 2021.

their high tempo operations. With the private sector and rival agencies competing for talent, Russia has spread their talent thin and have had to rely on purchasing malware from abroad and resorting to criminals for their talent.

Another weakness that stems from Russia's security practices is the rampant corruption that is exhibited by corrupt security officers. Media outlets were able to identify the FSB agents that were responsible for Alexei Navalny's assassination attempt from purchased data. We expect leaks in data to continue into the future as corruption remains prevalent in the Russian government. This corruption has even resulted in Russian government personnel being targeted by domestic hackers with leaks of their emails and correspondence exposing officers. So long as this corruption exists, we can expect future leaks in the future that shed further light into their operations.

Highlight on APT28

Evidence from analytical operations conducted by FireEye showcases APT28 to be highly politically motivated. Many of their targets include governments, militaries, dissidents and people opposed to the Putin-run Russian government. Their operations have consisted of information espionage campaigns to further the end goals of the Kremlin. They have carried out these operations in the conflict in Syria, in NATO-Ukraine relations, the 2016 U.S. presidential election, and many other instances. We also saw this group go after pharmaceutical and clinical organizations involved in COVID-19 research, most likely a directive from the Kremlin to attain a vaccine in a faster manner.

Looking at the way APT28 has been able to adapt over the years, we believe they will continue to prove a persistent adversary. The level of sophistication displayed in the programming of their malware showcases an elite force of programmers that can adjust to an evolving threat landscape.

Yet, the group is known to exploit known vulnerabilities, utilizing brute-force attacks to gain access to networks and data. Several agencies conducted an analysis of APT28's TTPs and found the group to be using a Kubernetes® cluster to conduct distributed brute force attempts against hundreds of government and private sector targets. APT28 also manages to take the easier route by employing a great deal of spear-phishing techniques, most recently targeting 14,000 Gmail users in late September 2021. Along with their use of Kubernetes® and spear-phishing, APT28 targets a significant amount of their activity towards organizations using Microsoft Office 365 cloud services. For government agencies with accounts tied to those services, they face the risk of being exploited.[2]

[2]Burgess, Christopher. "US and UK Issue Rare Joint Guidance in Response to Russian GRU Brute Force Campaign." *CSO (Online)*, 2021. *ProQuest*,

Yet the mitigation recommendations that come from top cybersecurity firms remain the same, ensuring multi-factor authentication, enabling time-out and lock-out features when password authentication is needed, employing appropriate network segmentation, and many other recommendations that have been vocalized many times before. But what is telling is that APT28 relies on container-orchestration systems for automating massive brute force attempts on systems. Similarly, depending on their ability to continue use of Kubernetes®, it is likely they will switch to other container-orchestration systems to continue operations such as AWS Fargate, Apache Mesos or Cloudify.[3]

Attacks Used by Russian Threat Actors

APT28: SERIOUS THREAT ACTOR (compromised Clinton campaign, DNC, DCCC in 2016)
Techniques used: Access Token Manipulation: Token Impersonation/Theft; Account Manipulation: Exchange Email Delegate Permissions (using Powershell to grant privileges to a compromised account); Acquire infrastructure domains (registered domains imitating NATO, OSCE sites); Large Scale Vulnerability Scanning; Boot or logon autostart execution: registry run keys/startup folder (deploying self-replicating malware to the startup directory for persistence)

- Essentially, a lot of brute force attacks, embedding malware into systems, and scanning for vulnerabilities and open source information. Might be worth looking into the trend in malware codebase to see evolution of sophistication.

APT 29: SERIOUS ACTOR (SolarWinds)
Techniques used: Abuse elevation control mechanism: bypass user account control; account discovery; account manipulation: additional cloud credentials; acquire infrastructure: domains. web services; vulnerability scanning; brute force: password spraying; email collection; Exploitation for Client Execution; Phishing: Spearphishing attachment and links; Spearphishing via **Constant Contact** (partner with Constant Contact for help discovering which accounts are associated with Russia and potentially easing tracing?); Supply Chain Compromise (Gained initial network access to some victims via a trojanized update of SolarWinds Orion software) -- a supply chain attack targets a third party with access to the organizations systems and codebase. (This is especially harmful to multinational companies and government agencies that have systems distributed in many regions)

---

http://search.proquest.com.ezp-prod1.hul.harvard.edu/trade-journals/us-uk-issue-rare-joint-guidance-response-russian/docview/2547776968/se-2?accountid=11311.

[3] (n.d.). (rep.). *APT28: AT THE CENTER OF THE STORM*. Retrieved from https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf?mkt_tok=ODQ4LURJRC0yNDIAAAGBMkq0JNuRQ5t4O3-K_1BfOoDgKynd-HfTXmb1fm2cVxsbpUk7Fy78oB3OSHVmKtEQz_1Z7G86-67SZT6CuuKJQ0qb9gf2JEtXQSuGbO6mhEXtw8U.

Attacks that worked against them:

-WannaCry in 2017: infected thousands of corporate and government networks.

-**NotPetya**: possibly designed by Russia and deployed against Ukrainian institutions but attacked many Russian networks.

Case Studies

With the following section, we will analyze the trends and patterns of Russian cyberattacks and espionage to understand similarities in approaches through different high profile incidents. To clarify the definitions used in this paper, cyber attacks are attacks that are malicious offensive operations that target computer systems for the purpose of damaging or controlling the system. They often manipulate some form of data, information, or networks in order to create the unwanted attacks. Cyber espionage, on the other hand, is just as invasive, but instead, does not particularly manipulate or damage specific systems. Rather it is more of a data breach in that it extracts particular information but does not overtly want to attract attention to itself in most cases. The goal is to gain information, not particularly to manipulate anything. Both activities are operations that Russia and Russian-linked groups have performed frequently and may cause significant unwanted consequences for the United States. The case studies that follow are a combination of both cyber attacks and cyber espionage, and our goal is to understand the methods utilized to create these operations as well as the patterns that underlie them.

One such example is the 2016 election DNC cyber espionage case. With this incident, the primary method used by Russian cyber operators was using phishing emails that went through the DNC to cause people to voluntarily give up their information.[4] One example would be having DNC staffers provide their credentials, which ultimately allowed the Russian hackers to gain access to 33 accounts whose data were later publicized through leaks.[5] By giving confidential credentials to the phishing scheme, Russian hackers were able to gain access to the email servers easily and quickly.

A second incident was regarding the SolarWinds cyber espionage operation. This operation involved hackers breaking into the SolarWinds systems to add malicious code to a program called Orion.[6] By having software that had been updated but tainted with a cyber security espionage program, the following update pushed out the code across the system, essentially creating an alternative bypass route for the hackers to access data and push further code.[7] The main service used, SolarWinds, had a lot of vulnerabilities to begin with, making it one of the loose links in the chain.[8] In addition there was a lack of leadership in the government and within

---

[4] Eric Lipton, Scott Shane, and David E. Sanger, “The Perfect Weapon: How Russian Cyberpower Invaded the U.S.,” The New York Times, December 12, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[5] CNN Editorial Research, “2016 Presidential Campaign Hacking Fast Facts,” CNN, October 13, 2021, https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

[6] “Solarwinds Hack Was 'Largest and Most Sophisticated Attack' Ever: Microsoft President,” Reuters, February 15, 2021, https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R.

[7] “Solarwinds Hack.”

[8] David E. Sanger, Nicole Perlroth, and Julian E Barnes, “As Understanding of Russian Hacking Grows, So Does Alarm,” The New York Times, May 28, 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

the company, which was one of the reasons which allowed the operators to be undetected for multiple months.

The connection between the Colonial Pipeline attack and Russia is less clear, but it also shows a similar pattern. The attack was reportedly caused by a leak of an old password without multifactor authentication which allowed for easy access into the VPN of the system.[9] This was not something that required high levels of technical ability, as it was just a password that had been found. The damages as a result of this hack were massive. Any longer and the supply chains would have been hit hard. And of course, many millions of dollars were paid as ransom and still much of it has yet to be recovered.[10]

A fourth example of cyber operations against a company was the FireEye cyber espionage case. In this example, some hackers were able to infiltrate FireEye, a top cybersecurity firm, and take some of its "Red Team tools," which allowed the company to help examine other organizations for cybersecurity weaknesses and vulnerabilities.[11] These were among the cutting edge of tools available for use and are securely guarded. However, as FireEye shared soon after, it was "an attack by a nation with top-tier offensive capabilities. This attack is different from the tens of thousands of incidents we have responded to throughout the years. The attackers tailored their world-class capabilities specifically to target and attack FireEye. They are highly trained in operational security and executed with discipline and focus. They operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past."[12] Based on further reports that they called the FBI, it seemed that Russia was the clearest potential actor, perhaps even its intelligence agencies. APT 29, or Cozy Bear, seems to be the agency most clearly linked.[13] Highly sophisticated espionage methods were used in order to gain access to important and valuable information.

These attacks and operations show a relatively clear trend as to the two types of patterns. For one, many hackers linked to Russia are not pursuing attacks of the highest technical expertise or pushing the boundary of cyber warfare. They are oftentimes not pursuing the newest technologies in a cyber race to see whether defenses can withstand the attacks. Instead, they are hacking through using more basic techniques like phishing and just password access, which are types of strategies that have been around for decades. And on the other front, there are other

[9] Sara Morrison, "How a Major Oil Pipeline Got Held For Ransom," Vox, May 10, 2021, https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.
[10] Morrison, "How a Major Oil Pipeline."
[11] Kevin Mandia, "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community," FireEye, December 8, 2020, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html.
[12] Mandia, "FireEye Shares Details."
[13] Lily Hay Newman, "Russia's FireEye Hack Is a Statement—but Not a Catastrophe," Wired, December 9, 2020, https://www.wired.com/story/russia-fireeye-hack-statement-not-catastrophe/.

cases like the SolarWinds cyber espionage case that are at the highest level of sophistication, pushing the frontier of cyber offense. There is less of a middle ground to the types of attacks/operations that are pursued. There are ones that are simpler, less sophisticated and likely more commonly used to target companies and organizations, and then there are also those that require significant new technical advancements that penetrate deep into the information bases. Typically the simpler ones are the cyber attacks, causing loss of control or damage, whereas much of the cyber espionage, which gains critical information (as opposed to physical/economic damage), uses cutting edge technology.

Recommendations

Based on this understanding, we recommend pursuing one initiative to reduce cyber risk, particularly pertaining to the first type of attack delineated, the less sophisticated but easily deployable ones. Because most of the successful operations are simply finding vulnerabilities that are already commonly known, as opposed to creating new vulnerabilities and offensive openings, USCYBERCOM should develop its own versions of similar attacks or operations and apply them to its own systems as a way to expose vulnerabilities clearly and quickly. Furthermore, this policy approach can be applied to the goal of reducing vulnerabilities in essential infrastructure in other government agencies as well as companies as a whole who may use it as a public service to bolster their own cyberdefenses. By turning inward and testing the US' cyberdefenses, USCYBERCOM can help reveal any gaps or pitfalls that it may itself have, or other important organizations may have.

Based on Russian capabilities and overarching technology trends, we expect the following to occur.

- We expect an increase in bot-net activity due to the advancement in computational power. More computational power can lead to the ability to coordinate wider botnet activity and direct those efforts for Denial of Service attacks. With increased computational power, we can also expect automated activity to increase. This means an increase in automated phishing emails, ransomware attacks and an increase in scanning networks.
- With an increase in disinformation campaigns, we must evaluate different levels of response to combat influence from the Kremlin. The problem doesn't really lie in curbing the number of disinformation campaigns, rather addressing the problem of "permissible environments", to counter them.
- Supply chain hacks that enable "capable adversaries to develop real-time espionage". We must understand all avenues that could lead the Russians into our networks. This means knowing every private company that has access to US Government networks or data.
- Keep emphasis on public-private partnerships
- We still recommend an emphasis on human personnel. Preparing personnel in government agencies to better implement cyber hygiene. Increasing the workforce to better analyze and implement offensive operations.

References

CNN Editorial Research. “2016 Presidential Campaign Hacking Fast Facts.” CNN, October 13, 2021. https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

Jibilian, Isabella. “The US Is Readying Sanctions against Russia over the SolarWinds Cyber Attack.” Business Insider, April 15, 2021. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

Lipton, Eric, Scott Shane, and David E Sanger. “The Perfect Weapon: How Russian Cyberpower Invaded the U.S.” The New York Times, December 12, 2016. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Mandia, Kevin. “FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community.” FireEye, December 8, 2020. https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html.

Morrison, Sara. “How a Major Oil Pipeline Got Held For Ransom.” Vox, May 10, 2021. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.

Newman, Lily Hay. “Russia's FireEye Hack Is a Statement—but Not a Catastrophe.” Wired, December 9, 2020. https://www.wired.com/story/russia-fireeye-hack-statement-not-catastrophe/.

Sanger, David E, Nicole Perlroth, and Julian E Barnes. “As Understanding of Russian Hacking Grows, So Does Alarm.” The New York Times, May 28, 2021. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

“Solarwinds Hack Was 'Largest and Most Sophisticated Attack' Ever: Microsoft President.” Reuters, February 15, 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R.