WORLD AFFAIRS COUNCIL
of Philadelphia

2020 Model Senate Foreign Relations Committee

Briefing Paper – Cybersecurity and Election Interference

Subcommittee on East Asia, The Pacific, and International Cybersecurity Policy

Topic Background

The ongoing technological advancements of the past three decades have revolutionized many economic, political and social structures, including the communications, banking, and transportation sectors. Today, billions of people across the planet rely on advanced technology and internet-based services to store personal information, connect with friends and family and shop for countless products. Increasingly, complex algorithms designed by technology companies push consumers toward everything from their next Amazon purchase, to new music and videos, and even personalized news and information.

Local, regional, and federal governments also increasingly rely on advanced technology for a host of services, from paying parking fines, to selecting health services and even registering to vote. However, over time we have seen these online systems hacked and manipulated causing significant economic, political, and cultural damage. In addition to the significant threat that **cyberattacks** pose on local, state and federal governments, **misinformation** campaigns and the rise of social media have further complicated our increasingly digitized life.

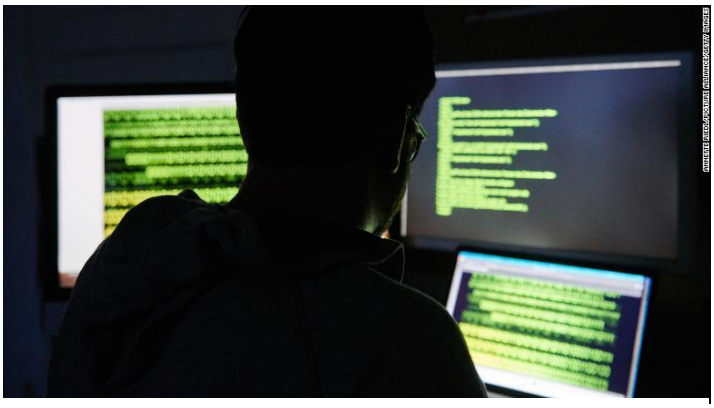

Photo: An anonymous man sits in front of three screens *(CNN Business).*

As technology has continued to advance and permeate through our lives, so too have the tactics of **hackers** and malicious actors. Hacking, once the domain of sci-fi films, is now a part of daily reality, and can cripple massive corporations and expose critical information of millions of individuals at any moment. Often, hackers target companies with outdated or under resourced **cybersecurity** operations and seek to either steal the personal information of consumers, or to **extort** the company for millions of dollars. However, with the rise of social media and the increasing spread of misinformation, cyberattacks have grown to include sophisticated campaigns used by individual and **state actors** to shape public opinions and influence votes.

Recent History: High-Profile Cyberattacks in the United States

Governments always have historically sought to shape political and other conditions around the world to their own benefit. Most recently, foreign governments have used cyberattacks and social media to influence the information environment in both Europe and the United States. Cyberattacks have become an increasingly common phenomenon in the United States, spanning both the public and the **private sector**. Both individual and state actors perpetrate cyberattacks for a variety of reasons, including

extorting money, stealing information, and even for the purposes of protecting national security. Thus, nations, corporations, and individuals have invested heavily in cyber security, as a means of protecting themselves from attack and building more resilient and defensive technological infrastructures. However, recent history has shown that increasingly sophisticated attacks, especially by state actors, means that even the best cyber defenses remain susceptible to crippling cyberattacks.

Within the last five years, the United States has seen several problematic trends relating to hacking and cybersecurity in the public and private realms. In 2014, hackers from a group called 'Guardians of Peace' hacked Sony Pictures to extort and intimidate the studio from releasing a film touted by the media as, "a far-fetched comedy about the assassination of North Korea's leader." [1] Although self-identified as a private group, the Guardians of Peace were eventually linked by U.S. intelligence experts as actors of the **autocratic** regime of North Korea. Administration officials at the time were hesitant to go on the record about intelligence findings and Sony opted for a digital release of the film after the hackers threatened additional attacks, possibly on theaters themselves, if the movie was released.

Photo: The City of Atlanta posted an outage alert on government related social media sites in 2018 *(Bank Info Security)*.

Additionally, in 2018, the city of Atlanta was the subject of a **ransomware** attack, where hackers took control of many municipal functions including online systems to related to the Atlanta Police Department, the judicial court system, and municipal infrastructure repair requests.[2] Although Atlanta refused to pay the hackers demands of $50,000, the city ultimately paid over 2.5 million dollars to repair and upgrade the hacked municipal systems. Other high-profile hacking incidents includes the 2013-2014 hack of Yahoo!, which exposed the accounts of all 3 billion Yahoo! accounts, as well as the 2016 hack of Uber, which exposed the personal information of 57 million users and 600,000 drivers.

Public and private entities have considerable opportunity to combat cyberattacks by implementing cyber security countermeasures. Cybersecurity has quickly grown into a multibillion-dollar global business, with firms partnering with almost every major corporation and local or state government to provide cybersecurity services. Many individual citizens, seeking increased digital privacy and security have turned to sophisticated cybersecurity defenses to protect their data and personal information. Likewise, large companies have begun to recognize consumer demand for digital security and have increased their commitment to protecting user data.

Although many hacking incidents can be financially motivated, some state-sponsored actors have turned to cyberattacks as a means of disrupting democratic discourse and influencing voters. These nefarious

[1] *U.S. Said to Find North Korea Ordered Cyberattack on Sony.* New York Times (2014).
[2] *Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare*. Wired (2018).

acts have included sophisticated attacks on state voter registration systems as well as coordinated social media campaigns meant to sew **disinformation** into the political discourse.

The Evolving Role of Social Media

The growth of social media represents a new frontier in the world of cybersecurity. Today, the world is more connected than it has ever been with more than four billion people engaged online and 3.5 billion on social media.[3] As mentioned previously, social media platforms allow for enhanced connectivity of users and mass communications. Often many individuals derive their news from social media, and trending topics could elevate opinions or raise issues to prominence. Using social media, politicians can speak directly to citizens, businesses can connect to consumers, and advocates can spread targeted messages to millions of followers. The growth of this sector has provided several challenges and opportunities.

Social media platforms like Twitter, Facebook and Instagram portray themselves as neutral platforms where users can choose to engage with content that appeals to them. However, this self-identified label leaves them with little editorial responsibility and essentially allows anyone to offer content, regardless of whether it is grounded in fact or fiction. Thus, many of these sites have experienced significant issues around mis- and disinformation, online harassment, and cyberbullying.

In recent years, these platforms have acknowledged their evolving role as a platform and have recommitted themselves to combatting misinformation and harassment in their services. In addition, many of these sites are flooded with a significant number of non-authentic accounts spreading messages and images with distinctly partisan lean. These **'bots'** are often used to drive conversations on specific issues, manipulate search results, enrage users and seed chaos. Facebook and Twitter are two companies who have recently made pledges to fight against bots and fake accounts that are directly linked to attempts to influence the American population.[4]

[3] *Mobile Technology and its Social Impact Survey*. Pew Research Center (2018).
[4] *Foreign Election Interference in the 2020 Race*. NPR (2019).

Election Interference

Issues around cybersecurity, social media and election interference in the United States came to a head with the 2016 U.S. presidential election. As many are aware, the United States underwent repeated cyberattacks leading up to the 2016 election. These cyberattacks included sophisticated hacking of state election offices[5], and state-sponsored disinformation campaigns waged on social media. It is important to note that there does not exist any evidence that any hacking campaigns directly changed or altered real vote counts, and that both experts and American policy makers disagree on whether the 2016 election was compromised in any way. However, an extensive online disinformation campaign, guided by Russia, has raised issues of foreign interference in a domestic election.

Photo: Former Justice Department Special Counsel Robert Mueller testifies before Congress *(C-SPAN).*

Russia's attempts to undermine the United States, its democracy, and its role as a global superpower come from a desire to return to its role as a global superpower, and its desire to uphold its autocratic regime. Since the cold war, Russia has shied away from outright conflict with the United States, instead choosing to engage in proxy wars, destabilizing efforts and international influence campaigns. One of the major strategies employed by Russian operatives is to sow chaos and division in Western societies, often attempting to drive a wedge between political parties. Experts warn that in theory, Russia is hoping to exploit President Lincoln's classic phrase: "A house divided cannot stand". Thus, Russia seeks to build itself back into a global superpower by dragging established democracies down.

Recently the Senate Intelligence Committee issued part two of a bipartisan report (co-authored by **Senators Mark Warner** and **Richard Burr**) finding that governments at all levels are unprepared to combat a Russian attack on U.S. election infrastructure. The reports suggest and endorse Special Counsel Robert Mueller's July 2019 testimony that Russian state actors knowingly made attempts to divide voters and cause U.S. citizens to have doubts about the integrity of American elections. Referencing the possibility of U.S. election interference in the future, Mueller warned during his testimony that "many more countries" could "develop an ability to replicate what the Russians have done". He also said that Russian attempts to interfere would most certainly continue in future elections when he commented, "they're doing it as we sit here," and "they expect to do it during the next campaign." As of January 2020, Senate Majority leader Mitch McConnell has refused to allow a vote on House-

[5] *Russia Hacked Voting Systems in 39 States before the 2016 Presidential Election*. Vox (2017).

passed election security measures, saying that such efforts are partisan and pointing to steps the Trump administration has taken to increase election security.

Subcommittee Charge

The Subcommittee on East Asia, The Pacific, and International Cybersecurity Policy is chaired by **Senator Cory Gardener** a Republican from Colorado and the Ranking Member is **Senator Edward Markey**, a Democrat from Massachusetts. The goal of this committee is to draft a resolution acknowledging the significant threats posed by individual and state sponsored cyberattacks on American businesses and local governments. The resolution should also focus on the potential threats of cyberattacks on American elections, including the hacking of voter registration and vote counting systems. Senators should seek expert testimony from a diverse group of witnesses on the current threats to the United States, including the principal aggressors, their geopolitical motives, and the technologies used to carry out attacks. Likewise, Senators should hear from expert witnesses on the ongoing opportunities to combat these threats including testimony regarding emerging technologies, sanctions or other policy tools. Expert witnesses should be prepared to provide Senators with relevant knowledge and policy recommendations. Expert witnesses should also be prepared to answer Senators' questions regarding their expertise in the field and nuanced understanding of the issue at hand.

Questions to Consider

1. Research one of the high-profile hacking cases listed above. Who perpetrated the attack, and what were they seeking?

2. Out of the '10 Types of Mis- and Disinformation' found in the infographic on Page 3, what types are the most prevalent in the United States? Provide a few recent examples.

3. According to your research, should the United States be concerned about the possibility of 2020 Presidential Election interference? Why or why not?

4. According to your research, what role do American companies and businesses play in terms of protecting citizens from cyberattacks? In comparison, what role *should* they play?

5. What role does social media play in terms of cybersecurity and the possibility of election interference?

6. What are examples of existing policies with regards to cybersecurity and preventing election interference that this subcommittee can endorse and/or build upon as a means of continuing 'best practices'?

Glossary of Terms

Term	Description
Autocratic	Relating to a ruler who has absolute power.
Cyberattack	Any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to a computer system, infrastructure network, or any other smart device.
Foreign Interference	An attempt to adversely affect, or undermine confidence in, any political, governmental, or democratic process, or prevent the exercise of human or democratic rights, through coercion, corruption, or the use of covert, malicious, or deceptive means, acting from abroad.
Disinformation	Wrong information spread with intent to deceive, confuse, and blur the lines, so that people don't know what to believe anymore. To prove that an incident counts as disinformation, it is necessary to prove both that the information was false and that the source spread it deliberately.
Misinformation	False information spread with intent that cannot be determined, or which can be shown not to be deliberate (e.g., if the source subsequently corrected itself).
hackers	A person who uses computers to gain unauthorized access to data.
extort	To obtain (something) by force, threats or other unfair means.
State-actors	A person (or group of people) who is acting on behalf of a governmental body
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Private sector	The part of the national economy that is not under direct government control.