Policy Briefing—Cyber Threats

Jonathan Stuckey

POLI-3160

Dr. Clary

Auburn University

2 October 2022

Executive Summary

With our society relying more heavily on technology now than ever before, our technological systems have become more secure, however, there still remains a large threat to the security of our country's institutions, businesses, and civilians due to potential cyber-attacks. As technological systems have become more intricate, so have the skills and accuracy of cyber attackers. Of the groups most likely to perform a cyber attack, the following are the most likely: **A foreign nation, a foreign independent actor or group, or a domestic independent or group.** However, it is important not to limit possible actors to just that group, as cyber attackers now can act in any form or size of group they wish. Industries and groups that are most susceptible to a cyber attack or cyberwarfare include, but are not limited to: **Government Institutions (especially the intelligence community and military operations), large corporations, and agriculture and health industries.**

Due to the severity that cyber attacks can cause on corporations, individuals, and the U.S. institution as a whole, it is recommended that the treat of cyber attacks be listed as a **vital interest** for national security policy-making decisions. As of now, there are no international laws or policies overseeing any part of the cyberspace, rather, policies and ethical codes are currently agreed upon by different technology companies when providing services, especially when they reside in different countries that operate under different laws. Domestically, there are a plethora of policies and laws that have been enacted to ensure safety for the cyberspace and technological infrastructures of large corporations and all federal government agencies. However, the threat of cyberwarfare still looms as a major potential threat, as we continuously increase our dependency on intricate technological infrastructures.

Cyber Terrorism

As part of our highly integrated society in the U.S., we are all now heavily reliant on modern technology and computers for daily functions for actions as simple as swiping a credit card, pumping gas, or arming our house security alarms. With our heavy reliance also come the major threat that cyber dependency poses. Ever since the beginning of technology integration in society, the threat of cybercrimes and terrorism has been present, with one of the first major international attacks being in 2005, when a group of Chinese hackers exfiltrated national security information from a Naval Air Weapons station, which included documents such as nuclear weapons test and design data, and stealth aircraft data (*Significant Cyber Incidents | Center for Strategic and International Studies*, n.d.). Since then, threats and attacks have become more common and sophisticated, with the threat of American intelligence being a target of attacks, including civilians personal information.

Threat Assessment

Of the countless threats we face as a nation today, none have increased to the level and with the speed that the threat of cyber warfare has. For that reason, it is recommended that the threat of cyberwarfare be listed as a **vital** threat and interest for the United States. Because cyber warfare should be seen as a vital threat, it is essential that the appropriate amount of resources be allocated to protect the vulnerability of our technological systems in the U.S. that help our entire society and government institution function.

No industry or individual is immune from the possibility of a cyber-attack, for example, from January to October 2021, more than 47 cases of a cyber-attack on a government agency were reported and 33 cases were reported from education systems (*Cyber Terrorism: What It Is and How It's Evolved | Maryville Online*, n.d.). In 2017, it was found that around $170 billion

was lost from American corporations due to cyber-attacks, which is around 0.87% of the America's GDP (*Cyber Terrorism: What It Is and How It's Evolved | Maryville Online*, n.d.). This number is expected to grow every year moving forward as it estimated that more than 80 billion malicious cyber activities take place every day across the world (*Cyber Terrorism: What It Is and How It's Evolved | Maryville Online*, n.d.).

What is cyber terrorism?

According to researchers, Jordan Plotnek and Jill Slay, cyber terrorism is "A premeditated attack or the threat of such an attack by nonstate actors intending to use cyberspace to cause physical, psychosocial, political, economic, ecological, or other damage. (*Cyber Terrorism: What It Is and How It's Evolved | Maryville Online*, n.d.)" The goal of a cyber-attack, often times, is for an actor to gain a sense of leverage over a government, corporation, or individual so that they can receive a ransom of some form or to act in a way that will be coercive to the attacked entity. For instance, one of the more notable and recent events, involved a Russian speaking ransomware group hacking the Colonial Pipeline, a major American pipeline, which required the oil company to pay more than $5 million in ransome (*Significant Cyber Incidents | Center for Strategic and International Studies*, n.d.).

In other situations, the cyber attacker is acting with the goal of stealing important and/or classified information to act maliciously. For instance, a nation or group of individuals may have an interest in performing a cyber-attack on a corporation or nation to cause harm, either for a political/power advantage or to receive something of monetary value such as a ransome. The information they receive from their attack and data breach will assist them in that goal. In other situations, the goal of a cyber-attack would be to destroy a technological system and its stored data, or to steal the information first.

Who can be attacked and what does an attacker look like?

Virtually any type of industry, individual, or government/nation is highly vulnerable to cyber-attacks and/or threats. Because our dependency on technology only continues to grow, so does the threat and the number of technological systems that can be affected. For example, it is expected that the growing usage of 5G networks, quantum computing, and artificial intelligence systems are all technological systems that are utilized in society today, but they are also systems that have opened our world to more potential threats, as cyber attackers have become more sophisticated in their programs that are able to search thousands of networks simultaneously to find weak and vulnerable spots to attack (Holmes, 2019).

One of the most difficult aspects of cyberwarfare is the identifying the attacker. Because our cyberspace is so vast and the traffic is so consistently heavy, identifying a cyber attacker is a very difficult task. Attackers can virtually live anywhere in the world, and in many occasions, the attacker may not be an identifiable person in the case that someone created an automated program to complete the attacks.

What are attackers trying to accomplish?

Almost any attacker, whether their target is a private citizen, or a government agency has the ultimate goal of causing harm—this harm is clearly defined and is rarely ever a random target and goal. Of the many targets that a cyber attacker could have in mind, **Government Institutions (especially the intelligence community and military operations), large corporations, and agriculture and health industries,** are at the biggest risk of experiencing an attack.

For large corporations, a data breach or ransomware attack is at the forefront of concerns for their leaders, as many of these industries contain vital personal information of millions of

Americans, such as bank account and Social Security information. In 2021, more than 1,291 cases of a data breach of a corporation were reported, and these breaches usually cost corporations $4.24 million in damages, along with the ethical damage caused by having their customers' information leaked (Lewis, 2018) (*Number of Data Breaches in 2021 Surpasses All of 2020*, 2021).

The ag industry is also not immune from the threat of cyber-attacks. During the 2021 harvest season, more than six major grain cooperatives experienced major cyber threats, which halted the entire ag supply chain for several weeks, causing major damage to agribusinesses around the country (Cox, 2022). This was a significant attack, because farmers only have a small window during planting and harvest season to work, as weather conditions are the most important factor to their work. Because of these cyber-attacks, many farmers were forced to miss that small harvest window, and by default, their yields were smaller and the entire supply chain was affected. As these threats to the ag community continue, we could experience larger threats to the ag supply chain as well as the entire American food supply.

Cyber warfare capabilities have been used to thwart major threats in the past, however, and were applauded by many nations around the world. For example, in 2010, an Israeli agent entered an Iranian nuclear facility to perform a cyber-attack to destruct their nuclear production. With a simple thumb drive, and a three-step process, the cyber attacker was able to halt Iran's nuclear production at the facility with a self-destructing program (Holloway, 2015).

Past and Present Policies Aimed at Cyberwarfare and Terrorism

International

Currently, there are no major international laws that help guide the function of cyberspace. However, as technological systems have grown over the past few decades, the

companies and creators of these systems have set in place ethical codes which have shaped the way that future technological systems are built and used. Many of these ethical codes are signed into action between companies as part of their contract when negotiations are made to access each other's technology for business.

Domestic

The protection of government technological systems is a vital effort, as they contain top secret information, as well as American's personal information. In 2017, President Trump signed a series of Executive orders and policies that help oversee the risk management systems of federal agency offices, including Executive Order 13800, which requires the heads of those agencies to submit a plan to the White House OMB that describes the way that their agency will spearhead cybersecurity (*Federal Information Security Modernization Act*, n.d.). These reports are submitted to the OMB quarterly.

In 2017 also, H.R. 2227, the Modernizing Government Technology Act, was signed, which granted federal agencies clearer direction and more funding to upgrade technological systems in an effort to have more secure systems (*H.R.2227 - 115th Congress (2017-2018): MGT Act | Congress.gov | Library of Congress*, n.d.). Additionally, this bill created the Technology Modernization Board who oversees the implementation of technological system upgrades throughout the federal government. This board routinely monitors the progress of each department's upgrades and can make funding and/or logistical assistance and recommendations if needed.

Analysis of Policy Options and Alternatives

International

One of the most prevalent issues that the lack of international regulation brings about is the fact that nations have no ethical limitations or guidance on how to use and/or respond to cyber tactics in time of war and combat. Additionally, if any future international cyberspace policies were to be implemented, there will be difficulties in the interpretation of the laws. These misinterpretations can be due to several reasons, but the most prevalent is that not all countries are as technologically advanced as others, and, therefore, there are large gaps between technological systems on the international stage which can create confusion when applying international cyberspace laws.

Last, one of the most difficult tasks of implementing international laws regarding cyberspace behavior is the enforcement of laws. Institutions such as the International Criminal Court lack unanimous international support, including the U.S., and therefore, it would be difficult to have a unanimous international agreement on an international cyberspace oversight system. Also, the process of monitoring international cyberspace activity is so difficult because of the sheer amount of cyber activity and also due to the fact that actors in the cyberspace are very difficult to attribute an identify to.

A way to educate and positively influence the international cyberspace, without necessarily creating new international laws would be to create an international technology governance board. Through this governance board, leaders from around the world would be able to share pertinent information about the success of different domestic cyberspace practices and regulations that have been implemented in their country. This board could also assist in the technological growth of developing nations. Last, this board could assist international and domestic technology companies by sharing their research, expertise, and advice in best international cyberspace practices.

Domestic

Because federal agencies, especially within the intelligence community, are under a constant threat of data breaches and cybersecurity threats, it is extremely essential that protocols are in place to ensure that there is oversight and investigations into these events when they occur. Additionally, by having quarterly reports submitted to the OMB, agencies can be held to a higher sense of accountability, allowing for a less likelihood of data breaches and cyber-attacks. What EO 13800, specifically, fails to address:

- Any possibility of increases in funding for cyber security prevention,
- Increased security standards for more high-security agencies such as the CIA, FBI, and military agencies

The most notable benefit of a policy like the Modernizing Technology Act is that it is designed to upgrade government agency technological systems to create a less vulnerable system, being that many of these agencies store top secret information and American identity information as well. The Technology Modernization Board is made up of seven voting members who represent different areas of the government. The benefit that having those members specifically is that each area of the government can be represented which means that they will have a higher likelihood of receiving the funds and assistance they need to improve their systems.

One of the issues that could evolve from the Technology Modernization Board is that domination by one government agency over others may occur due to different needs of each agency. An event like this could be the product of or potentially cause interagency conflicts, which could then have a negative impact on the efficiency of our national security agencies. Last, the voting members are members who are experts in the field of technology and general

national security, therefore, there may be government agencies and/or industries that are not represented as well. For example, there are no members who represent the health care, agriculture, or energy sectors, which are proven to be large targets for cyber attackers.

References

Cox, J. (2022, June 13). *Agriculture Industry on Alert After String of Cyber Attacks*. Government Technology. Retrieved October 2, 2022, from https://www.govtech.com/security/agriculture-industry-on-alert-after-string-of-cyber-attacks

Cyber Terrorism: What It Is and How It's Evolved | Maryville Online. (n.d.). Maryville Online. Retrieved October 2, 2022, from https://online.maryville.edu/blog/cyber-terrorism/#examples

Federal Information Security Modernization Act. (n.d.). CISA. Retrieved October 2, 2022, from https://www.cisa.gov/federal-information-security-modernization-act

Holloway, M. (2015, July 16). *Stuxnet Worm Attack on Iranian Nuclear Facilities*. Stanford. Retrieved October 2, 2022, from http://large.stanford.edu/courses/2015/ph241/holloway1/

Holmes, A. (2019, October 1). *7 Emerging Technologies That Cybersecurity Experts Are Worried About*. Business Insider. Retrieved October 2, 2022, from https://www.businessinsider.com/7-emerging-technologies-that-cybersecurity-experts-are-worried-about-2019-10

H.R.2227 - 115th Congress (2017-2018): MGT Act | Congress.gov | Library of Congress. (n.d.). Congress.gov. Retrieved October 2, 2022, from https://www.congress.gov/bill/115th-congress/house-bill/2227

Lewis, J. (2018). *Economic Impact of Cybercrime*. McAffee. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Number of Data Breaches in 2021 Surpasses All of 2020. (2021, October 6). Identity Theft Resource Center. Retrieved October 2, 2022, from https://www.idtheftcenter.org/post/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/

Significant Cyber Incidents | Center for Strategic and International Studies. (n.d.). Center for Strategic and International Studies |. Retrieved October 2, 2022, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents