Cyberwarfare: The Wild Wild Web

Wessly Soronellas

Cybersecurity Institute, Kennesaw State University

CYBR 7050: Cybercrime Detection, Analysis, and Forensics

Gang Lee, Ph.D

May 2, 2021

Abstract

This paper dives into the current topic of cyberwarfare. This includes what is considered cyberwarfare and what is considered a cyberattack, what is the appropriate response to a cyberattack according to international law, and what are some current examples of cyberattacks. Moreover, this paper identifies the lack of legislation regarding cyberwarfare and why such discussion needs to be made urgently. Some key take-aways from this paper include how cyberwarfare has evolved with limited accountability and who was influential in its creation.

Keywords: cyberwarfare, cyberattack, cyberterrorism, SolarWinds, United Nations

Cyberwarfare: The Wild Wild Web

Technology is not a new concept. Some of the first technological innovations created by humanity included creating weapons from rocks and sticks as well as the ability to start a fire by generating enough heat created by friction. A brief history of humanity shows an instinctive drive to adapt to the environment by means of innovation. Periods of technological advancement such as the industrial revolution evolved society to become more reliant on technology for survival the ever before. The same is true today in the digital age of society. As more children are growing up emersed in technology, the reliance on its functionality is inevitable. Physical real-world objects can communicate and be controlled through an internet connection. While these advances provide tremendous opportunity to better society, there is also room for exploitation from malicious actors. As more critical infrastructures in society become digitalized and connected, nations must also take steps to defend national security and prevent these critical infrastructures from being compromised by foreign adversaries. This process has created a new battleground for nations to indirectly start wars on other nations with limited terrestrial presence. Recent events such as the SolarWinds breach as well as previous breaches like Equifax and Stuxnet demonstrate the lack of legislation that governments have on international diplomacy regarding internet activity. Moreover, more events will continue to occur if there is no response; therefore, to continue to advance society in an amicable manner whilst also reaping the benefits of these technological advances both foreign and domestic there must be a discussion on cyberwarfare. This includes discussing the potential impacts cyberattacks have, defining cyberwarfare and the asymmetric advantages it provides, and theorize what an appropriate response to a cyberattack might look like.

Literature Review

Impacts of Cyberwarfare. Cyberwarfare can affect the physical world via the use of the internet and/or software. Such an example can be seen from the United States' successful cyberattack against Iran's Natanz uranium enrichment plant where the "goal was to physically destroy a military target-not just metaphorically, but literally." (p 1, Langner, 2011) When discussing the impact of the cyberwarfare weapon, Langner writes:

> While a computer program only operates on information, a controller program-sometimes called *ladder logic*-operates on physics. This is an interesting and important point, especially for cybersecurity considerations: manipulations of a controller have less to do with the confidentiality, integrity, and availability of information and more to do with the performance and output of a physical production process. In the worst case, controller manipulations could lead to physical damage. Stuxnet was the worst case, as it was carefully designed by experts to do just that with the utmost determination.

While there are numerous samples of military cyberattacks causing physical damage in the real world, Stuxnet was a historical event that set the tone for foreign interreference via cyberwarfare. In terms of societal impact of cyberwarfare, the […]"dependence-vulnerability nexus is true not just for the military but for society at large, as vital civilian infrastructures are run by industrial control systems that are exposed to cyberattacks." (McGraw from Simone Dossi page 6, 2020) In addition to civilian industrial control systems, these critical infrastructures may also include examples like […]"the electric grid, communication and transportation networks and financial services [where] if these 'strategic weak points' are hit, society as a whole will be paralyzed." (pp. 12-13, Shaojie et al. from Dossi, 2020) Power grids allow communities to inhabit areas of extreme temperatures with the use of heating and air conditioning; however, an attack that shuts down the power grid not only paralyzes society but also threatens the lives of those living in harsher climates across the United States such as Arizona in summer or New York in Winter. These types of attacks, while still cyberwarfare, are "a form of cyberwarfare that specifically targets vital civilian infrastructure" called 'information and infrastructure warfare.'

Defining Cyberwarfare. Cyberwarfare is in its infancy in comparison to traditional war; therefore, there is a lack of definitive language that outlines what qualifies to an act of war in cyberspace. For example, in the United Nations "International customary law (legal norms that have been developed through state practice), now codified in UN Charter Article 2(4), provides that states are prohibited from engaging in the use of force. […] Although no precise definition exists for the term 'use of force' under international law, most experts agree that it includes cyberattacks that cause physical damage or injure individuals." (p 1, Boothby et al., 2012) This language defines (albeit vaguely) what is categorized as a cyberattack. Despite expert's agreement on general terms of what defines a cyberattack, there is the lack of a universal definition for cyberwarfare because "[t]here is no multi-national treaty which refers to cyberwarfare, so cyberwarfare has many definitions. It can be defined as 'warfare conducted in cyberspace through cyber means and methods.'" (p 6, Avci, 2016) This lack of legislative discussion has enabled nations to attack and exploit foreign networks with no accountability. Recent cyberattacks performed by nation state actors include the SolarWinds incident, documented as the largest widespread breach in history, which is believed to be an attack from one of Russia's intelligence agencies APT 29 or Cozy Bear (Nakashima & Timberg, 2020). Equifax, a large crediting agency, also encountered a large breach which compromised more than half of the American population's sensitive information including social security numbers, data of birth, and home address. The Equifax investigation led to findings that tied the responsible actors to be performing on behalf of the Chinese government. Historical hacks such as these two examples highlight a common trend of less developed countries attacking superior countries via cyberwarfare due to the asymmetrical advantage smaller countries have in attacking in cyberspace compared to a traditional terrestrial war. Because of this asymmetrical advantage smaller countries have in attacking more technologically superior countries such as the United States, deciding on an appropriate response is difficult.

Responding to Cyberattacks. Responding to cyberattacks is a difficult decision to make especially when deciding on behalf of a nation. A logical process might be to analyze the incident in terms of questions such as who was behind the attack, what was the motivation for the attack, and what impact did that attack cause? The answers to these questions, if known, can help in determining an approach that will limit the possibilities of war and unnecessary death but also provide a stern response that prevents future incidents. According to Article 51 of the UN Charter on the right to self-defense as a response to an armed attack states that the "…Charter shall not impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations…," however, the charter "…does not clearly define armed attack." (p 7, Avci, 2016) Because of this lack of definition, it is hard to determine "what conditions will provide the threshold of an armed attack and when cyber attacks can be considered as an armed attack under Article 51." (p 7, Avci, 2016) Despite the lack of definitive language in what categorizes a cyberattack as an armed attack, most experts agree that "…it is reasonably clear that the term, 'armed', in the Article 51 includes kinetic or electronic attack, both having the capability of having the same results." Therefore, a cyberattack can be classified as an armed attack and allows self-defense as a response. When discussing a response to an armed attack the UN states that if "[t]he Security Council [have] authorized a Chapter VII response, [omit] UN- or US-initiated sanctions, armed self-defense, and belligerent reprisal can be examples of lawful responses. Additionally, countermeasures such as legal responses, access controls, could be added to these options." (p 15, Avci, 2016) Most nations prefer to avoid armed conflict if necessary, therefore,

> "[a]nother option is that of applying pressure on a state without the use of armed force.[…] After a threat to the peace, breach of the peace, or act of aggression has been determined under Article 39, the Security Council can call for measures under Article 41 of the UN Charter. Such measures can be economic or trade, which do not involve the use of armed force, to international military action such as embargoes, travel bans, financial or diplomatic restrictions." (pp. 16-17, Avci, 2016)

While armed responses are lawful in the event of an armed cyberattack, these responses may not result in the most effective solution as armed conflict will most likely lead to casualties and a disruption of peace; therefore, when responding to an armed attack an effective response might be economic or trade that provides a monetary impact while preventing unnecessary casualties.

Findings

Defining cyberwarfare leads to a similar definition to that of cyberterrorism. In Yar and Steinmetz's book on 'Cybercrime and Society,' they reference Verton's definition of cyberterrorism as "the execution of a surprise attack by a subnational foreign terrorist group or individuals with domestic political agenda using computer technology and the internet to cripple or disable a nation's electronic and physical infrastructures." (p 88, Yar & Steinmetz, 2019) Moreover, the authors challenge the legitimacy of cyberterrorism concern in stating that "[p]erhaps more so than any other form of cybercrime, however, internet terrorism is bound up with, and often obscured by a great deal of rhetorical embellishment and myth-making. […] It has been suggested by more skeptical commentators that there is little empirical evidence to warrant the level of concern currently being generated over cyberterrorism, nor to justify the sweeping enchancemen5t of state powers that are being instituted in order to respond to the supposed threat." (pp. 93-94, Yar & Steinmetz, 2019) While this position on cyberterrorism being a moral panic and an excuse for governments to increase their power, the ongoing discoveries of cyberattacks performed by nation-state actors has proved those concerns as valid.

Equifax. There are several cyberattacks that have occurred recently that highlight the legitimacy of cyberterrorism as well as the real-world impacts of cyberwarfare that provide actual examples of attacks rather than theoretical situations. Despite the large civilian population affected by the 2017 Equifax hack, approximately 145 million Americans personal identifiable information (PII), this incident can be found as politically motivated and therefore undermines the overall purpose of highlighting the legitimacy of cyberattacks and its relation to cyberterrorism. Therefore, the Equifax hack shall be considered an alleged attack from a Chinese-sponsored group, but the incompetence demonstrated by Equifax and the politically motivated accusation of Chinese involvement result in this example to not be rendered applicable for this discussion. (Berghel, 2020)

Stuxnet. The sophisticated worm created to attack Iran's nuclear facilities that resulted in malfunction and failures of nuclear centrifuges demonstrate the legitimacy of cyberattacks. This incident can be viewed as cyberterrorism because it was the result of a conscious attempt to damage a facility that can be identified as a critical infrastructure. Though the United States and Israel are believed to be the responsible parties, both countries have denied being involved. This assumption is based on the complexity of the technology developed and implemented as well as the political motivation regarding Iran's nuclear production. It's important to mention that cyberterrorism is a politically motivated event that attempts to attack a country or individual based on political motivation; therefore, Stuxnet is a great example of a cyberattack and its relation to cyberterrorism. (Montgomery, 2019)

2016 United States Election. In the case 18-cr-00215-ABJ United States of America v. Netyksho et al., the Grand Jury for the District of Columbia charged the defendants on a count of conspiracy to commit an offense against the United states which states:

> "In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted largescale cyber operations to interfere with the 2016 U.S. presidential election." (U.S. Department of Justice, 2018)

This cyberattack led to the breach of confidential emails of then Presidential candidate Hillary Clinton where the emails were released to the public via WikiLeaks. Many believe that these released emails played a major role in the election of Donald J. Trump. When discussing cyberterrorism and a cyberattack, this example documents the legitimacy of cyberattacks being performed out of political motivation. Moreover, the confidence in the election process was severely damaged since the 2016 election; therefore, the decreased confidence in the democratic process played a significant role in the capitol riot that occurred on January 6th, 2021. (Piore, 2019; Schaake, 2020)

SolarWinds. Using a supply-chain attack, hackers were able to embed malware into legitimate updates for the IT monitoring platform from SolarWinds. Because SolarWinds programs are a popular choice for IT performance management in both the private and public sector, the hack has found to have "…targeted at least nine federal agencies and at least 100 private-sector businesses." (Gaouette, 2021) While this hack is believed to be an espionage mission, the size of targets has officials concerned like deputy national security adviser for cyber and emerging technology Anne Neuberger who stated "when there is a compromise of this scope and scale, both across government and across the U.S. technology sector . . . it's more than a single incident of espionage. It's fundamentally of concern for the ability for this to become disruptive." (Nakashima, 2021) Therefore, this attack can be categorized as a cyberattack due its scale of organizations affected. However, the current information regarding the SolarWinds hack limits the ability to determine the attack as a form of cyberterrorism as the political motivation is yet to be identified.

Discussion

There is much to digest given the information provided in the previous passages, but there are two key take-aways that are most important to remember. First, there are several examples of countries interacting in the cyberspace that can be categorized as a cyberattack and/or cyberterrorism, yet there has been little to no responses from targeted victims though the UN Article 51 supports self-defense given the event of an armed attack. There has been a recent update from the United States as a response of the SolarWinds hack where "[t]he Biden administration is preparing sanctions and other measures to punish Moscow for actions that go beyond the sprawling SolarWinds cyberespionage campaign to include a range of malign cyberactivity and the near-fatal poisoning of a Russian opposition leader." (Nakashima, 2021) While this is an important action that will set an example for any future cyberattacks, the most recent action is the first nonarmed response the United States has had against Russia despite numerous examples of meddling. Because of these events, the discussion of cyberterrorism as a moral panic and an excuse to increase government power can be determined to be false. While these statements may have been true in the past, the current political climate has used technology more frequently to advance political agendas with cyberattacks and cyberterrorism.

Another important take away, and perhaps the most important of the two, is the United States' responsibility in creating this toxic environment. While China and Russia have both been identified as performing state-sponsored attacks against the United States, the United States was the first to use a cyberweapon (Stuxnet) to attack a country's critical infrastructure (Iran's nuclear facilities) for political reasons; therefore, the United States, though not formally identified as responsible for building Stuxnet, are the first documented country as performing cyberterrorism. In addition to the introduction of cyberwarfare, the United States has used cyberspace for political purposes. As seen in the Equifax breach, the Department of Justice's indictment of four Chinese soldiers can be seen as a political stunt due to the late nature of the report and the lack of responsibility placed on Equifax's lackadaisical security framework. Moreover, the Council of Europe's Convention on Cybercrime (Budapest Convention) was another example of politically motivated behavior from the United States can be seen "…[i]n 2019, the United Nations (UN) began debate of similar treaty [Budapest Convention] initiated by Russia that included contributions from China, Australia, Canada, Cuba, the United Kingdom, Japan, and several other allies." (p 4, Berghel, 2020) Because China and Russia were those in charge of its creation, the U.S. did not move forward to ratify the treaty. The critique on this American ideology further details that:

> "[t]he U.S. demand that it be immune to accountability suggests that a more accurate term be American exceptionalism. As long as such nationalistic attitudes prevail, it will be difficult to get all prospective international criminals to unite behind cybercriminal

> activity, and as a consequence of this will be that the United States will remain an attractive target." (p 4, Berghel, 2020)

Therefore, there must be criticism towards the United States as well in the creation of this current climate of cyberwarfare.

Policy Implications

Government Procurement. Going forward there are several options available to further reduce the occurrences of cyberwarfare. The first of which can be to strengthen security networks by government regulation. Bruce Schneier discusses the overall structure of security is flawed by stating "…the software that's managing our critical networks isn't secure, and that's because the market doesn't reward security. Schneier further proposes that the first step is government software procurement:

> "Software is now critical to national security. Any system of procuring that software needs to evaluate the security of the software and the security practices of the company, in detail, to ensure that they are sufficient to meet the security needs of the network they're being installed in. If these evaluations are made public, along with the list of companies that meet them, all network buyers can benefit from them. It's a win for everybody." (p. 2, Peisert et al., 2021)

Government procurement would result in a transparent market that would influence companies to invest in security as more secure companies would be rewarded with higher consumer confidence.

International Legislation. In addition to government regulation, an international treaty ratification that clearly states inappropriate behavior in cyberspace as well as providing accountability through enforcement. However, because these attempts have already been proposed in the past, it’s clear that in order for future attempts to be successful China, Russia, and the United States must compromise on the structure. This is much easier said than done, but the need for international compromise in cybersecurity is critical in advancing society for future generations.

Conclusion

This paper provided insight into the various sections of cyberwarfare from a western perspective. This includes mentioning recent cyberattacks that have occurred against the United States as well as cyberattacks performed by the United States (allegedly). Additionally, the definition of cyberattacks and cyberwarfare was given and what a lawful response might look like according to United Nations international law. The several examples of cyberattacks were used to highlight the legitimate presence of cyberwarfare as well as to provide motivation to take steps to reduce future occurrences. As technology continues to integrate with the physical world through the internet of things (IoT) as well as increasing network communication speeds such as 5G wireless networks, there will be more opportunities for malicious actors to use this technology to cause harm to society. As a result, it is important for nations to come to an agreement to try and prevent such harmful attacks from occurring.

References

Avci, Maya Ezgi. "A LAWFUL RESPONSE TO CYBER ATTACKS," no. 12 (2016): 35.

Berghel, Hal. "The Equifax Hack Revisited and Repurposed." *Computer* 53, no. 5 (May 2020): 85–90. https://doi.org/10.1109/MC.2020.2979525.

Boothby, William H., Wolff Heintschel von Heinegg, James Bret Michael, Michael N. Schmitt, and Thomas C. Wingfield. "When Is a Cyberattack a Use of Force or an Armed Attack?" *Computer* 45, no. 8 (August 2012): 82–84. https://doi.org/10.1109/MC.2012.282.

Caldera, C. (2020, November 28). Fact check: Fairness Doctrine only applied to broadcast licenses, not cable TV like Fox News. USA Today. https://www.usatoday.com/story/news/factcheck/2020/11/28/fact-check-fairness-doctrine-applied-broadcast-licenses-not-cable/6439197002/.

Dalsheim, Joyce, and Gregory Starrett. "EVERYTHING POSSIBLE AND NOTHING TRUE: NOTES ON THE CAPITOL INSURRECTION." *Anthropology Today* 37, no. 2 (April 2021): 26–30. https://doi.org/10.1111/1467-8322.12645.

Dossi, Simone. "On the Asymmetric Advantages of Cyberwarfare. Western Literature and the Chinese Journal *Guofang Keji*." *Journal of Strategic Studies* 43, no. 2 (February 23, 2020): 281–308. https://doi.org/10.1080/01402390.2019.1581613.

Ellen Nakashima, C. T. (2020, December 14). "Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce." *The Washington Post*. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.

Gaouette, N. (2021, February 20). “White House says it will hold those responsible for SolarWinds hack accountable within weeks.” *CNN*. https://www.cnn.com/2021/02/19/politics/sullivan-solarwinds-khashoggi/index.html.

Langner, Ralph. “Stuxnet: Dissecting a Cyberwarfare Weapon.” *IEEE Security & Privacy Magazine* 9, no. 3 (May 2011): 49–51. https://doi.org/10.1109/MSP.2011.67.

Library of Congress. (n.d.). Amdt1.3.1 Freedom of Press: Overview. Constitution Annotated. https://constitution.congress.gov/browse/essay/amdt1_3_1/.

Montgomery, Maxwell. “PROLIFERATION OF CYBERWARFARE UNDER INTERNATIONAL LAW: VIRTUAL ATTACKS WITH CONCRETE CONSEQUENCES.” *Southern California Interdisciplinary Law Journal* 28 (n.d.): 24.

Nakashima, E. (2021, February 24). “Biden administration preparing to sanction Russia for SolarWinds hacks and the poisoning of an opposition leader.” *The Washington Post*. https://www.washingtonpost.com/national-security/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fa-e0ccb3660358_story.html?source=content_type%3Areact%7Cfirst_level_url%3Anews%7Csection%3Amain_content%7Cbutton%3Abody_link.

Netyksho, Viktor Borisovich, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, and Aleksey Viktorovich. “UNITED STATES OF AMERICA,” n.d., 29.

Peisert, Sean, Bruce Schneier, Hamed Okhravi, Fabio Massacci, Terry Benzel, Carl Landwehr, Mohammad Mannan, Jelena Mirkovic, Atul Prakash, and James Bret Michael. “Perspectives on the SolarWinds Incident.” *IEEE Security & Privacy* 19, no. 2 (March 2021): 7–13. https://doi.org/10.1109/MSEC.2021.3051235.

Piore, A. (2019). Hacking 2020. *Newsweek Global*, 173(3), 20–33.

Ruane, Kathleen Ann. “Fairness Doctrine: History and Constitutional Issues,” n.d., 17.

Schaake, Marietje. “The Lawless Realm: Countering the Real Cyberthreat.” *Foreign Affairs* 99, no. 6 (November 2020): 27–33. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=eoh&AN=1870088&site=ehost-live&scope=site&custid=ken1.