Innovation to the Future of Cyberwarfare

(Technical Paper)

Government Response and Role in the Social Construction of Cybertechnologies

(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Huy Huynh

Fall, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____Huy Huynh_____ Date __5/10/2022__

Huy Huynh

Approved _____ Date _____

Rosanne Vrugtman , Department of Computer Science

Approved _____ Date _____

Sean Ferguson, Department of Engineering and Society

Introduction

This prospectus will focus on cybersecurity and cyberspace. Data and information have begun moving to a digital format at an exponential rate. With this shift to a more online and cyber world, this leads to more potential cyberattacks and overall more cyberwarfare. My technical topic is about my internship at Two Six Technologies, and about working on an innovative project named Project IKE to help visualize cyberspace. The main objective of this project is to create a platform where attacks and defenses in cyberspace can be mapped out digitally, and artificial intelligence can help suggest the user to decide about whether an attack or defense can be successful or not. This project can help search and also develop information on targets. It can also obtain large amounts of information and use that information with machine learning to become an integral part of cyberwarfare.

With the technical topic of Project IKE, this leads into the STS topic about cybersecurity and its effects on the world over the past decade. The social construction of technology will be focused in the analysis of the government and affect company actions of ill-natured cyberattacks. This relates to Project IKE as a reason behind this project development is because of the growing number of small scale and large scale cyberattacks.

Technical Topic

In the cybersecurity field, there has been a lack of planning tools for cyberwarriors, people who are involved in the attack or defense of information systems. Cyberattacks and defenses were difficult to plan and having such a planning tool will save a lot of time (Pomerleau, 2019). Over the Summer of 2021, I had the opportunity to be an intern at Two Six Technologies and was able to work on Project IKE, a software that was meant for this type of planning.

At the internship, I helped develop Project IKE. Project IKE is a planning tool for cyberwarriors, where battle plans can be created and saved. It can also take in data and utilize it to even suggest an action plan if cyberwarfare is recommended in certain situations. It's expected that this program is going into a larger initiative called Joint CYber Command and Control, or JCC2. A Department of Defense spokesman stated that "Project IKE is an artificial intelligence-enabled tool which will provide a new way for cyber forces to understand the common operating picture" (Pomerleau, 2019).

During my time at Two Six Technologies, I helped upgrade the program's Java version by updating Dockerfiles and YAML files, and made a custom JDK to save space. The upgrade helped Project IKE be more up to date and be more compatible with potential new features added. I then wrote a custom flag in a terminal command when calling for data in Project IKE. This new custom flag will extract all the column information in the SQL database and return it to

the user in a dictionary. Lastly I also added an API rate limiter to prevent too many people from accessing the program.

From this experience, I realized the importance of cybersecurity and cyberwarfare. As time moves on, data is gradually moving to be stored digitally. This leads to people with malicious intent to steal information from others, which then leads to the growth of cybersecurity to keep cyberspace safe for everyone. This research paper will delve into the field of cybersecurity and cyberattacks.

STS Topic

Over the last decade, there have been an increasing number of cyberattacks. These cyberattacks range from small email phishing to large scale shutdown of big companies. They have begun to be an issue in the past and are still a problem to this day. The first large-scale ransomware attack on companies was the WannaCry attack on May 17, 2017, where old Windows computers' data was stolen for ransom (Gregory, 2021). Another example is a more recent and bigger ransomware attack on Colonial Pipeline in May of this year, which halted Colonial's actions in distributing gas. The shutdown of the gasoline pipeline system was a major impact of the ransomware attack, leading to many worldwide effects of higher gas prices and gas outages. Furthermore, Colonial decided to pay the ransomware of $4.4 million after the attack, which unfortunately incentivizes even more hacker groups to continue these cyberattacks (Turton, 2021). Given the growing alarm of potential large-scale cyberattacks, in this research

paper, this paper will use the social construction of technology to explore the actions that the government have taken to try and counteract these attacks. This paper will also aim to investigate the government's values of the importance of cyberspace, their concerns with the safety within cyberspace and their views on the significance of cyberspace in the future.

With the increasing rate of cyberattacks, the government had to begin to label things a bit more differently and seriously. International Relations Scholar Myriam Dunn Cavelty has analyzed the new social construction of cybertechnology within the government. In her article she stated that "cybertechnologies are treated like any other tool of power projection and coercion", meaning that after the massive uptick in cyberattacks, the government began to view cybertechnoglies as not just a piece of digital technology, but more of an important political issue in general (Cavelty, 2018). The government realized the importance of cyberspace and treated it as a political issue, which is more than just technology. The social construction of cybertechnologies is morphing into something of more importance than before because of the growing rate of cyberattacks.

In a doctorate thesis written by Semire Yekta, they mentioned the use of the social construction of technology in relation to cyberspace in their thesis about "Online Fraud". They mentioned that "one of the most important characteristics of cyberspace is the construction of a unique form of connectivity" (Yekta, 2019). They quoted Mlambo's belief that the "Internet is a network of networks, and these networks are interconnected to each other in different configurations". The author uses sources from Mlambo and Holt to talk about how cyberspace is this social construct where individuals can engage with one another despite being in different

locations. Yekta's explanation of cyberspace in regards to the social construction of technology reveals that this new social construct is still very underdeveloped and how it is currently exploited through online fraud and crime. Yekta also said that it "in turns creates a unique environment and engenders challenges that cannot be solved through traditional crime prevention and detection methods", which also shows how common practices of fighting against cyberattacks will not work in this new social construction of cyberspace (Yekta, 2019). The author's use of social construction of technology in relation to cyberspace relates to this paper's topic about the alarming rate of cyberattacks and lack of protection against them since cyberspace is still a new social construct in development.

The government is affected greatly by this growing rate of cyberattacks. There is plenty of sensitive data within the government and potential attacks to obtain them will hurt the government. Although, the US government isn't doing a good job at defending against cybersecurity attacks mainly because of it being difficult to defend and their apathy for cybersecurity. There are so many entry points where an attacker can come from, so the smaller scale companies will also have to participate themselves and upgrade their own securities to ensure safety. From the McKinsey & Company's book on the transformation of cybersecurity, they have talked about potential ways to fight back against these attacks. The book stated that the government is able to take initiative by enforcing companies and organizations to have necessary cybersecurity requirements (Digital, 2019). In a 2019 Congressional report on the US Federal Government, the Committee on Homeland Security and Governmental Affairs investigated eight agencies within the government and found a long list of vulnerabilities. In many cases, the agencies even lacked government certification that their systems were in proper working order

(Senate, 2019). Two years later, the Committee on Homeland Security and Government Affairs investigated the same eight agencies and they identified many of the same issues they found (Senate, 2021). From these studies, it is clear that the US government has a lack of care for the cybersecurity of their systems since 2019. Despite there existing potential actions from McKinsey & Company's book, the government has not taken much initiative in the fight against cyberattacks in the past. However, on May 12th, 2021, President Joe Biden issued an executive order to improve the nation's cybersecurity. In the executive order, he wanted to modernize cybersecurity defenses in the country by having open channels for sharing information on cybersecurity and to enforce cybersecurity requirements on organizations to prevent further damages. Federal agencies are also expected to modernize their technology environment and security practices (The United States Government, 2021). There have been attempts in the past, but this attempt has better potential as the executive order called for updated authentication and encryption frequently and planned timelines for implementing and monitoring each federal agency and their technology environment (The United States Government, 2021). This executive order did not have much criticism as the focus on cybersecurity became more important. This is a strong example of the government finally stepping up after recent large scale attacks such as the Colonial Pipeline attack. Over time, the government has had apathy towards cybersecurity, but with the recent attacks, worry of future attacks, and the consequences behind them, the government is beginning to see the social construct of cybertechnologies as an integral part of their system. The theory of the social construction of technology asserts that the improvement of cyberdefense as a system is still being constructed by the growing rates of cyberattacks and the consequences from them.

Next Steps

In regards to the technical topic, the next steps for Project IKE would be to continue to develop how it will analyze its data and use it to even be able to suggest actions to the user in relation to cyberwarfare. With Project IKE already being able to organize attacks and defenses in cyberspace, focusing on how AI can use the data within the program to suggest the best actions in a cyberwar will be beneficial to government officials that may use it.

For the STS topic, the government has only just begun their actions on improving the cybersecurity within the government and companies outside the government. The next step for the government would be to analyze if the executive order by Joe Biden was the right move in strengthening cybersecurity. It is currently too early to notice any huge effects of the new regulations. Once these regulations become solidified and effects begin to occur, steps can be taken to even further strengthen the cybersecurity regulations. Potentially stricter timelines and more frequent checks to find vulnerabilities can improve the new executive order even more.

References

Cavelty, M. D. (2018). *Cybersecurity Research Meets Science and Technology Studies* (thesis). Cogitatio, Lisbon.

Digital McKinsey and Global Risk Practice. (2019). *Perspectives on transforming cybersecurity*. *McKinsey & Company*. Retrieved October 17, 2021, from https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx.

Fryer-Biggs, Z. (2020, September 13). *Twilight of the Human Hacker*. Center for Public Integrity. Retrieved October 17, 2021, from https://publicintegrity.org/national-security/future-of-warfare/scary-fast/twilight-of-the-human-hacker-cyberwarfare/.

Gregory, J. (2021, September 1). What has changed since the 2017 WannaCry ransomware attack? Security Intelligence. Retrieved October 4, 2021, from https://securityintelligence.com/articles/what-haschanged-since-wannacry-ransomware-attack/.

Pomerleau, M. (2019, November 27). *Cyberwarriors lack planning tools. that could change.* Fifth Domain. Retrieved October 17, 2021, from https://www.fifthdomain.com/dod/2019/11/25/cyber-warriors-lack-planning-tools-that-could-change/.

Senate., Portman, R., & Carper, T., Federal Cybersecurity: America's DATA AT RISK: Staff report (2019). Committee on Homeland Security and Governmental Affairs.

Senate., Portman, R., & Peters, G., Federal Cybersecurity: America's data still at risk: Staff report (2021). Committee on Homeland Security and Governmental Affairs.

The United States Government. (2021, May 12). *Executive order on improving the nation's cybersecurity*. The White House. Retrieved October 17, 2021, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Turton, W., & Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg. Retrieved October 4, 2021, from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-usingcompromised-password.

Yekta, S. (2019). *The social construction of online fraud* (thesis).