Thesis Project Portfolio

Innovation of Cyber Defense Technologies with Data Analysis and Collection

(Technical Report)

How have past cyberattacks affected how different social groups use and interact with software technology today?

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Michael Kosar

Spring, 2023

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Cyber attacks and crime have risen exponentially in the past decade. The global reliance on technology to store data, perform daily tasks, and function as a society has enticed malicious hackers to exploit these often weak systems and their vulnerabilities. One such entity that is constantly under attack from adversaries is the United States Air Force. The majority of their equipment relies on digital systems and transmissions in order to function which makes them vulnerable to cyber attacks from adversaries. Specifically, their equipment can be jammed via certain radar waves that are sent to disrupt their signals. To address this problem, I created a way to be able to identify the difference between normal, everyday radio-waves that are harmless to defense systems and the malicious adversarial radio-waves being sent by potential adversaries to disrupt communications. I did this through a combination of computer programs and data analysis in order to sort, compile, and display data to make this distinction. It is important to consider the human and social dimensions of this because the U.S. government is tasked with defending its citizens and if they cannot properly do that, then there can be serious consequences.

From an STS perspective, we can analyze the broader question, how have past cyberattacks affected how different social groups use and interact with software technology today? We can use the social construction of technology theory to analyze this question by determining how different social groups have affected how our software is developed currently. To conduct this research, I will use four different case studies of real cyber attacks and analyze the attack, consequences, and impact on society. In this, I hope to learn from these past attacks and use the information gathered to analyze how they have affected our approach to software development today. In turn, we can decipher where we have failed in the past and use these lessons to better secure our future. Together, both the technical project and STS research have

real implications. They provide both an analysis of what we have done in the past to solve the problem of cyber security and an example of what we are doing currently. This can give us an insight into what we can do in the future by looking at our current technology and learning from our past mistakes in order to create a safer and more secure future.