Thesis Project Portfolio

Utilizing Artificial Intelligence, Data Analytics, and Machine Learning to Strengthen Cybersecurity Infrastructure

(Technical Report)

Analyzing Cybersecurity Infrastructure in the United States: Effectiveness of the Current Structure

(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

Andrew Chau
Fall, 2023
Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Cyber crimes could cost the world $10.5 trillion annually by 2025. My technical report aims to propose a design in implementing new innovative technologies into the cybersecurity infrastructure in order to help mitigate cyber crimes and attacks. My STS research focuses on exploring the similarities and differences in the United States and EU's current cybersecurity infrastructure and using that information to determine whether the current system in the United States should be changed. The relationship between the two projects are correlated where after researching how detrimental cyber crimes are to people and companies it made sense to explore a way on how to implement change into these systems to help mitigate the attacks.

The technical portion of my thesis produced a proposed design of a system that utilizes machine learning, data analytics, and artificial intelligence to help cybersecurity systems detect and deal with threats more effectively and efficiently. The first distinguishing feature of my system is the machine learning aspect where it takes existing data and uses it to train itself on patterns on what is considered "normal" and "abnormal". Another key feature is using artificial intelligence for real-time threat detection and response where it will continuously monitor and adapt to change in order to swiftly identify and respond to anomalies and reduce response time in an emergency. Lastly, data analytics is used to gain a deeper understanding of trends by processing and extracting insight from vast amounts of existing data, such as logs, events, and user behaviors, and feeding the conclusions to the machine learning algorithms. This proposed design aims to strengthen cybersecurity infrastructure by implementing more diverse and technologically innovative threat mitigation tools and techniques.

In my STS research, I looked at the current structure of cybersecurity infrastructure in the United States in response to a rise of cyberattacks in cyber physical systems over the past several years. Ultimately, the question was whether or not the current task force established by the Federal Government in dealing with cybersecurity was effective in doing its job or if it needed to be revamped. Discourse analysis was used to conduct a cross cultural comparison of the EU's policies, infrastructures, and plans in regards to combating cyber crimes and how they approach cybersecurity. This allowed for a gain of a wider perspective and an insight of ideas that could be implemented and adopted in the United States. The biggest influence in differences between the two countries' approaches was the cultural aspect of prioritizing cost-benefit in the United States. It is of high importance and often outweighs other factors, whereas, the EU focuses primarily on the safety and wellbeing of the people they aim to serve over cost and profit. Therefore, the analysis provided a better understanding of why the current infrastructure is the way it is and can help highlight areas of importance to consider when proposing new policy or revamping agencies.

Both my STS research and technical report aim to help the people who either use these systems or put their trust in providing personal information to them since companies often lack accountability when people are not aware of their wrongdoing. This ties back into the concept from *Hurricane Katrina: One year later: What must we do next?* by Andersen et al., where they go back and dissect the faults in the system and propose plans about what could be done differently or improved upon in order to prevent something catastrophic like that from happening again. My research provided context and background on why the current system is the way it is and makes the audience aware of the situation, while my technical report provides one proposal to improve the system so that some of these faults can be mitigated. In both the reading and my own work, the people are at the forefront of importance rather than cost.