Sociotechnical Synthesis

Modern society is deeply intertwined with modern technology, and the reaches of the internet extend into nearly all aspects of life. As more and more of our personal data is stored electronically, the risks of losing that data or having others access that data grows increasingly dangerous. Whether it is financial information or photo albums, internet users have the right to protect their data at all costs, but this may be easier said than done. To dispel attacks, companies and government agencies collect data and employ surveillance measurements to ensure that data is being protected and virtual services are being used properly, but the balance between effective security and over-intrusive surveillance is hard to maintain. With better policy and the introduction of successful cybersecurity programs driven by machine learning, cyberattacks may be better protected against without any infringements upon user privacy.

The technical component of this project aims to investigate how machine learning can improve security in electronic systems. By having algorithms or procedures that can easily and accurately identify and prevent cyberattacks, systems can better protect data and prevent intrusions. Using the MITRE CALDERA cybersecurity framework, advisories and defenders can be simulated to model cyber attacks and prepare defenses for these attacks. Adversaries are equipped with abilities that can be set up with tactics, techniques, and procedures, or TTPs, detailing how an attack will be carried out. Agents, which can be advisories or defenders, can be placed in groups with each group working to attack or defend. The defending agents are equipped with abilities to defend against various attacks and the abilities are constantly updated to better recognize and prevent attacks.

The STS component of this project focuses on the use of surveillance in remote work environments. As many companies take steps to protect their data, employees are increasingly

being monitored to ensure they are not putting company data at risk and to encourage maximum productivity. This has raised concerns as employees feel as though their privacy is being violated and they must compete with employers to find a balance. Due to the COVID-19 pandemic, many companies shifted to remote work environments, and with a lack of in-person monitoring, many employers introduced virtual surveillance measures that extended the reach of employers further into the personal lives of employees. Policy changes both on the company level and government level must be implemented to protect the rights of employers and clearly define the jurisdictions of private and public corporations.

This project aims to highlight the flaws and successes of current cybersecurity protocols a well as investigate the ethical issues related to protective surveillance measures. These issues must be considered not only by engineers in the related fields but also by policy makers and employers so that privacy on the internet can be strictly maintained.

I would like to extend my gratitude to my advisors, Professors Peter Norton, Sean Ferguson, and Jack Davidson for their support and guidance throughout this project.