Thesis Project Portfolio

Cybercriminal Network Building: An Automated Solution to Cyber Threat Analysis
(Technical Report)

The Intersection of Ethics and Artificial Intelligence in U.S. Federal Cybersecurity: An In-Depth Analysis
(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

Kevin Michael Carlson
Spring, 2024
Department of Computer Science

Table of Contents

Sociotechnical Synthesis

My thesis project consists of a technical project paper and a sociotechnical research paper. My technical project paper describes the work my team of five people completed during my internship in the summer of 2023. My team and I were challenged with developing an application for automating cyber-threat analysis. Cybersecurity analysts often only have access to individual data nodes when responding to a detected threat and connecting these nodes to potential threat actors is a labor-intensive process in a time-sensitive environment. My team and I developed an end-client application for generating meaningful connections between a queried data point and filtered datasets using a refined clustering algorithm. Our solution utilized an in-house, synthetically generated Personally Identifiable Information (PII) dataset to represent a reasonably practical dataset available to the client. We employed a density-based spatial clustering of applications with noise (DBSCAN) algorithm to automatically develop multi-level relationships between nodes, with the end product displaying these results in graphical interfaces. Given several test cases, our model correctly identified 89% of related data points when queried on a single PII attribute (e.g. blockchain address, MAC address, email). The project's next steps involve expanding the potential data types to be handled by the algorithm and further refining the recognition of relationships by exploring other means of clustering information.

My sociotechnical research paper focuses on the increasing overlap between federal cybersecurity and artificial intelligence through the lens of ethics. The escalating cyber threats faced by the United States government have surpassed human capabilities, prompting the exploration of artificial intelligence (AI) into the federal cybersecurity landscape. This paper conducts a comprehensive ethical analysis of the employment of AI in nation-state governments around the world, as well as analyzes the current climate of AI in the US and what the

intersection between such a revolutionary technology and cybersecurity will bring. As national cyber security strategies increase the employment of AI, the need for a defined ethical framework becomes imperative for aligning societal values and agency agendas.

I implored an ethical analysis of current literature relating to the use cases of AI in national governments worldwide. As with the global comparison of many national policies under the lens of ethics, the public-facing literature is diverse and constantly evolving. The European Union, with its proposed "EU AI Act" establishes a holistic regulatory framework categorizing AI applications based on risk levels. In contrast, China emphasizes the preservation of socialist values through monitoring content, training data, and data labeling, as outlined in its Interim Administrative Measures for Generative Artificial Intelligence. The broad objectives of ethical regulations in AI are considerably influenced by national agendas, while still acknowledging shared principles among them. Furthermore, this paper will delve into the existing AI ethical discourse in the US, highlighting key contributors such as the American Artificial Intelligence Initiative launched by President Trump in 2019. Through the research conducted, the conclusion was made that, while the US leads the global market in AI start-up company metrics, the country remains passive in terms of regulatory engagement.

The convergence of AI and cybersecurity introduces a plethora of ethical challenges, requiring meticulous consideration. This paper identifies eight core ethical principles related to responsible AI: privacy, accountability, safety, transparency, non-discrimination, control of technology, responsibility, and promotion of human values. In evaluating current literature, the primary principles that most effectively address the integration of AI into cybersecurity were found to be privacy, bias, and transparency. This paper focuses on these three attributes when discussing the enhancement of AI ethics within US federal cybersecurity. My findings point

towards the implementation of a rights-based ethical framework. The prioritization of the American public's well-being is of utmost concern to ensure the maintenance of public trust and relevant ethical obligations. This type of framework will also immediately reconcile public doubts about the use of AI applications in national cybersecurity that have risen from previous media coverage. Artificial intelligence is currently an unbounded technology with unforeseen ethical risks in the future. I also suggest ethical documentation be rolled out on an agency-to-agency basis so the role of synthesizing relevant ethical guidelines of the mission and use cases that each cybersecurity agency has can be tailored accordingly. My research paper may serve as a reference point for ethical policy-making in federal cybersecurity agencies looking to employ new AI technologies in their missions.