Thesis Project Portfolio

How Do We Teach Cybersecurity?: Cybersecurity as an Interdisciplinary Study at the University of Virginia

The Undiscussed Civilian Victims in the Crossfire of Cyberwarfare

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

Samuel Y. Ahn

Spring, 2024

Department of Computer Science

Contents of Portfolio

Executive Summary

How Do We Teach Cybersecurity?: Cybersecurity as an Interdisciplinary Study at the University of Virginia

The Undiscussed Civilian Victims in the Crossfire of Cyberwarfare

Prospectus

Executive Summary

Cybersecurity is a massively, rapidly developing field in computer science as technologies further advance and the need for securing digital assets become more apparent with the dangers of cyberattacks and risks of confidential information leaking to malicious actors. With computers increasingly intertwined with almost every aspect of people's lives, so increases the potential cyber vulnerabilities present in their lives. The technical report portion of the thesis will be focused on cybersecurity education in higher education, specifically with improvements to the UVA School of Engineering and Applied Science Department of Computer Science's undergraduate cybersecurity curriculum. The STS research paper portion will focus on the impact of cyberwarfare between nation-states on the civilians of targeted societies. This thesis aims to highlight the importance of cybersecurity as an essential part of software engineering, the field of computer science, and establishments with computer technologies from education to human-machine interactions at a global, societal scale.

In the technical report of the thesis, the problems of specifically UVA Computer Science's cybersecurity curriculum are outlined, and potential solutions for improving the curriculum are presented. The issues of the current cybersecurity curriculum consist of issues with the effectiveness and efficiency of teaching cybersecurity theory and skills, teaching ideologies and methodologies, retention of content, preparation for real-world application post-academia, and lack of significant undergraduate certification opportunities. Changes to the current curriculum to address these problems aim to improve general cybersecurity education by improving the depth of understanding of curriculum content, acquiring a real-world applicable skillset for the field, and gaining the value of proper recognition and qualification for their investment into the curriculum at UVA through better structuring of the cybersecurity

curriculum. With these improvements, the department can better utilize students' time investments and offer better opportunities for the students inside and outside of school. The proper education of the next generation of computer scientists in cybersecurity is crucial for the future.

In the STS research paper, a deeper developing topic in cybersecurity is covered with a specific focus on the human-machine interaction of civilians caught in cyberwarfare taking place between nation-states. One of the most important developments in computer science would be the constant evolution of cyber powers at high levels of government used for intelligence, espionage, and warfare. With the world increasingly integrating every aspect of life with computers, from banks and public transit to power grids and communications, these aspects of life become vulnerable to cyber-attacks. As such, nation-state actors have begun to weaponize cyber tools to exploit these vulnerabilities to accomplish the agenda of the state, whether that is to ransom the computers of unsuspecting victims to fund the government or shut down the power grids to bring an entire nation to a stand-still. While the cybersecurity world pays close attention to the direct damages and political impacts of cyberwarfare, the direct impact on individual civilians caught in the crossfire is seldom focused on, and there is not much anthropological research being done to deeply understand the physical, social, and psychological impact on civilians targeted on behalf of their governing body. The STS research hopes to compile existing literature on the topic and act as a contextualizing primer for cyberwarfare to prepare future works for exploring the topic.

The research into these two topics throughout the year serves to propel cybersecurity in academia and the general public. The work put into the capstone research hopes to instigate a discussion within the UVA Department of Computer Science to not only streamline and enrich

the cybersecurity curriculum but also then further re-evaluate and integrate the important field of cybersecurity as a core, integral part of computer science education at the school where I, myself, learned computer science from scratch. The STS research paper highlights a major and significant aspect of cybersecurity, cyberwarfare, which seems to have a lack of work done in the more anthropological research on the effects of a new kind of warfare on the welfare of affected civilians. The work in compiling information from the few scattered articles that care more about the societal impact of cyberwarfare hopes to encourage and call to action further research into a newly emerging, unprepared, ethically gray, and unrestricted type of warfare to better understand, mitigate, and prevent the potentially grave consequences that follow suit. I believe that I successfully achieved what I set out to do in academia, as well as put forth a significant thesis that serves the furthering of cybersecurity awareness and education, an important factor to consider in every area of work and study.

I would like to thank Professors Daniel Graham and Aaron Bloomfield for helping me realize my passion for cybersecurity, teaching and guiding me through my time at UVA CS, and providing me the opportunity to be a teaching assistant for the cybersecurity courses and gain more insight into the field and education of cybersecurity at UVA.