

Thesis Project Portfolio

Innovation to the Future of Cyberwarfare

(Technical Report)

Government Response and Role in the Social Construction of Cybertechnologies

(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

Huy Huynh

Spring, 2022

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Innovation to the Future of Cyberwarfare

Government Response and Role in the Social Construction of Cybertechnologies

Prospectus

Sociotechnical Synthesis

My research addresses the problem of growing cyberattacks and lack of cybersecurity in the United States. In order to solve this issue, I worked with Two Six Technologies and helped work on Project IKE, a tool for visualizing cyberspace. Attacks and defenses can be mapped out digitally through this software and artificial intelligence can be used to advise the users on how to go about a cyberattack. Since cyberattacks can attack anyone at any scale and can lead to large consequences, the issue of cyberspace affects society as a whole worldwide. It is a growing problem that could get out of hand if not dealt with early in its development. This issue can be seen through an STS perspective of the Social Construction of Technology (SCOT) framework. SCOT focuses on how technology is shaped over time through a variety of social factors and this issue involves how cybersecurity itself is constructed over time. I will use historical research to analyze cybersecurity by using past examples of attempts of government intervention in cybersecurity and previous cyberattacks. I also want to draw upon SCOT and use that to better understand how cybersecurity was developed over time in order to find potential solutions to the issue and why this issue exists in the first place. Cybersecurity is still an undeveloped technology, so I expect to find information about how there is still a sense of apathy in relation to the subject from the government and from different companies as well. Implications from Project IKE and my STS research include the increasing reliance on online information. A lot of sensitive data is transferring from paper to digital and that leads to more attempts at cyber attacks to obtain that information. These attacks are growing at an alarming rate, and with analysis of the SCOT of cybersecurity, Project IKE can be used as a way to visualize this cyberspace and be a reliable way to fix this problem.