# An Analysis of the Impact of International Cyberwarfare Interactions Between Nation-State Government Actors

**STS 4500 Prospectus**

**Department of Computer Science**

**B.S. Computer Science**

**The University of Virginia, Charlottesville**

**Name: Samuel Ahn**

**Technical Advisor:**

**STS Advisor:** Alice Fox

**Projected Graduation Date: 05/2024**

**Submission Date: 05/12/2023**

# International Cyberwarfare Interactions

## Overview:

The main question of this technical project asks what the extent of the impact of cyber interactions between nation-state? Cyberwarfare would include any act of using cyber technologies to disrupt a state or organization. This could be using cybersecurity exploits to convey espionage for a nation-state. My connection to this topic would be my personal interest in cybersecurity as well as the cybersecurity focal path I am pursuing for my undergraduate computer science degree. One cool thing that I hope my readers will learn from my work is how cyber interactions play a great role in impacting our lives without even knowing that it is present in many unexpected places, and have a better awareness and understanding of how greater bureaucracies are directing societies through cyber interactions that fulfill their own agendas.

## Positionality:

As the first generation only child of a Korean father, I grew up in a part of a urban-leaning suburban area of Virginia close to D.C. in a large mixing pot of immigrants and white Americans. The schools were well funded and highly diverse with a relatively large student body, and the students, teachers, and parents, highly progressive. I am grateful to understand that my upbringing was a peaceful one full with opportunity and sheltered from discrimination or ostracization, and I grew up learning the many different cultures and experiences of many different people. I was surrounded by many different political beliefs both radical and moderate towards both sides of the spectrum, and taught by those who could teach with without bias.

That being said, I was ignorant of the very different lives of the people who lived elsewhere in the country with different environments and situations. I do not have the experience of those who grew up with financial hardships, so I may not understand the limits of not being able to afford something that I take for granted. I do not have the experience of those who have faced discrimination, and therefore, I may not understand which certain actions have unintended consequences leading to unfair bias, nor may I understand how these biases can vastly change a person may respond. As a political moderate myself, I may understand the views and perspectives of those whose ideas differ from mine. But despite these differences, I try to understand and account for the perspectives I have not had experience with for not only as an engineer, but as a person so that I can better understand, empathize, listen others, and perceive the world and my work from another's point of view.

## Problematization:

The main problem of my project topic would be the impact of international influence on societies in order to fulfill a personal agenda, often detrimenting the target society. There is also controversy on whether or not cyber technology exploitation should be used to carry out certain goals due to the damage it can cause and its necessity in national security. The main actors would be specifically the departments of government overseeing cyber actions, third-party sourced organizations, and the upper level bureaucracy enabling and commanding these interactions to

happen, some examples including: the CIA, responsible for multiple offensive cyber operations against multiple Middle Eastern states, Nobelium, a Russian government-backed hacking group responsible for the SolarWinds hack, and President Trump, the POTUS that authorized and directed the CIA to launch more cyber operations.

Primary plot points addressing the three main categories would be shown through case studies. An example of cyber warfare: Russia's hack on the Ukrainian power grid attempting to blackout a large portion of Ukraine during a standstill of the ongoing Ukrainian War; an example of cyber espionage: the Titan Rain hacking by Chinese military hackers that attempted to steal data from the U.S. and U.K.; for an example of social engineering, the usage of social botnets acting as users on Reddit spreading Russian propaganda on social media such as Reddit during the Ukraine War.

**Guiding Question:**

The main question of this project is, "What is the extent of the impact of cyberwarfare between nation-states on the civilian population of these bodies?"

**Projected Outcomes:**

My research aims to bring together different acts of cyberwarfare from various countries and analyze the impacts of cyber attacks on the societies that are targeted, as well as other societies that may have been victimized.

**Technical Project Description:**

My technical project will delve into a specific type of cyber attack that utilizes a malware known as a worm. A worm is a specific form of malware, slightly different than a virus, that, once it enters a network through a single vulnerable machines, will propogate through that network and all of its machines. These infected machines can then be programmed to further spread the worm through whichever network it connects to, and be exploited in various ways; being used as ransomware, completely disabling the machine to disrupt the network it is a part of, or secretly being added as another node in a botnet, or a web of many machines that can be used for malicious purposes.

**Preliminary Literature Review & Findings:**

There are numerous articles on the affects of cyberwarfare in scientific lenses that are both STS and outside of STS, but many disclaim of the validity of their contents as time goes on as cyber technologies, cyberwarfare, cyberspace itself and its definition, and real-world capabilities are constantly evolving, either by deprecating, upgrading, and increasing its already expansive areas of use.

There are more than plenty sources outside of scientific papers on the topic of cyberwarfare documenting allegations, actions, and impacts of acts of cyberwarfare through media sources such as news outlets, online forums, social media, and press releases. These sources are less reliable and extremely susceptible to bias and inaccuracy, but should be mentioned and analyzed through a very thorough and cautionary lens, as these sources show, and

can even be a part of the impact of these cyber actions on groups of people. These sources are also the most concurrent at the cost of accuracy, but can still hold legitimacy through journalist sources, cybersecurity and STS specialists, and sometimes direct information from the government actors in question such as the FBI, CIA, and DHS in only the United States (although these government releases should also be viewed with skepticism as there is often no release or even attempts of formal investigations, and governments are known to purposely exclude information or give out false information to prevent self-incrimination or leaking of sensitive information).

By analyzing and compiling articles into one paper, I can contribute by adding more documentation to a field where concurrent information is scarce with general, high-level, and easily digestible information.

The biggest concern when researching a topic related to cyberwarfare interactions between nation-state bodies is following the early actions of larger superpowers such as the United States and Russia, is that nations have been extremely conservative about releasing or confirming their information, technologies, and activities until their declassification decades later. Most research is hidden within layers of government clearance and secrecy. That being said, there are few scholarly articles that are up to date, backed by strong evidence, are relevant to current cyberwarfare, and are even accurate as the definition of cyberwarfare is constantly changing and the field ever expanding. It is presumed that these government agencies are more advanced in technological power, and that we as the scientific community do not know of most of their current activities, but we can analyze the effects of concurrent and concluded acts of cyberwarfare through their impacts on civilians and societies from an STS perspective.

**STS Project Proposal:**

The goal of this project is to analyze how the effects of cyberwarfare between two nation-states affect the civilians of the nations involved. This project is designed with the idea of outlining how the cyber interactions between nation-state change societies by showing how individuals, groups of people, environments, and relationships are affected by the cyber actions and the possible implications for the future they bring.

For this particular project, the method of approaching the objective of the project is to view the affects of cyber interactions with a focus on societal impacts. A large portion of why I believe the research on cyberwarfare interactions is that the impacts of these operations are not simple such that they are isolated to only the agents involved, the target objective of interest, and the extraction of intelligence. In reality, since these acts of cyberwarfare impact nation-states' governments, naturally the people are also affected in politics, military, ideology, and favor and resentment. In these acts of cyberwarfare, there is bound to be collateral damage that can affect the safety, privacy, and livelihoods of innocent civilians. Cyberwarfare can also affect the environment these societies inhabit drastically through disablement and destruction. It is because the actions of these nation-state bodies affect the innocent civilians involved for the agenda of these government groups and desired consequential outcomes, either intentionally as a part of

their schemes or accidentally as collateral damage, either beneficially or detrimentally for the society, that this is a highly STS issue.

The approach for this project is grounded around ANT as the project primarily focuses on the impacts of specific actors, such as the government bodies and other organizations, civilians, technologies related to the cyberwarfare, and the technologies used by civilians, and the different networks of relationships between these actors. With the project's objective being outlining the causes and effects of cyberwarfare interactions, ANT is a sufficient and convenient method to analyze these relationships and outcomes.

The anticipated methods to use to properly convey this analysis is through the literature review of existing scholarly resources on the subject of cyberwarfare and specific cyberwarfare related events (both STS and non-STS articles) along with narrative analysis of the literature involved.

A somewhat unconventional approach to help construct the analysis on top of literature review would be to present case studies of specific cyberwarfare interactions through multiple media artifacts including, but not limited to, news media articles on these specific events, interviews of parties involved, such as firsthand and secondhand accounts of relevant actors in the *Darknet Diaries* podcast, and official statements by government organizations.

Although these resources are usually not suitable for a literature review or scientific papers due to the a large room for inaccuracy due from multiple factors such as biases, hearsay, potential falsification, differing and opposing claims and standpoints, and personal agendas, I believe that when these sources are analyzed conjunctively as opposed to individually while scrutinizing carefully and inquisitively, and accounting for biases, the sources may reveal general yet accurate information regarding the state of concurrent cyberwarfare events as well as the impacts they have on the societies associated with them. This method is also a way to compensate for the lack of literature across this topic and credible, official published information by nation-state organizations responsible for these actions.

**Barriers & Boons**

The two main barriers to this project would be my inexperience with this kind of work as this is my first experience with writing a literature review as well as my first time writing a paper with an STS focus. It is also my first time viewing this topic through the actor network theory method, meaning that there is room for error with my lack of mastery over the subject.

On the topic of actor network theory, although it may be a good method to identify the relationships between the actors within this subject, not all of the people, institutions, and technologies are identified (some records may have been lost, may be incomplete, or may be unreleased to the public), so there may be a significant relationship that may be difficult to establish and point out.

On the topic of cyberwarfare in STS, there are relatively few scholarly resources available on this topic because of its highly specialized nature, obscurity, and lack of data and information. The existing papers may also be outdated due to the nature of the information

regarding this topic being withheld by governments until their declassification, which is often in the range of decades of years. The existing papers may also be outdated due to change in definitions of terms in cybersecurity, cyberspace, and cyberwarfare, and the chaotic nature of how these groups operate.

In order to address the lack of experience with writing a literature review on an STS topic, I plan on speaking with my STS professors and resources within my university institution as well as doing further research into STS methodologies and theories using online resources.

For my lack of knowledge in the field of cybersecurity regarding specific information on how these interactions take place and the technology behind them, as well as cybersecurity theory and practices, I plan on speaking with my cybersecurity Professors at my university institution and interview them on their own research on these topics.

To compensate for the lack of reliable resources on this topic for more modern and contemporary events, I plan on using online media sources to attempt and form case studies analyzing the cyberwarfare event itself as well as the impact it has on society.

## References

*A History of Cyber Security Attacks: 1980 to Present* (2016)

Bruce Middleton, a cybercrime specialist and international speaker describes the major recorded cyber attacks and hacks from nation-states and independent organizations. Middleton describes these cyber attacks from 1980 to 2016 including Stuxnet and Sandworm (NotPetya). Middleton is generally objective and unbiased as he explains the history of these various attacks with a focus on major nation-state like the U.S. and Russia. This resource can be used to help assess the span of these attacks while also giving the context and the aftermath.

*Darknet Diaries, Episode 54: NotPetya, Russia vs. Ukraine: The Biggest Cyber Attack Ever* (2023)

Jack Rhysider, a cybersecurity knowledge professional and SecOps worker hosts an episode of *Darknet Diaries*, discussing the story of Sandworm, or NotPetya, a very powerful worm that affected all of Ukraine and caused millions of dollars in damage with author of *Sandworm*, a detailed account of Sandworm from multiple perspectives, written by a Wired Magazine reporter, Andy Greenberg. The podcast goes into detail with topics from the book, *Sandworm,* with multiple firsthand accounts of cybersecurity experts and government officials during the Sandworm attack. This podcast and book are very useful in

determining the affect of the Ukrainian and world population due to a cyberwarfare attack by Russia.

*Digital Blood on Their Hands: The Ukrainian Cyberwar Attack (First Edition)* (2023)

Andrew Jenkinson, a U.K. cybersecurity professional with experience as CEO of multiple security companies writes about the cyberwarfare attacks against Ukraine from Russia since the China Winter Olympics, describing the affects of these actions of cyberwarfare and arguing that Russia started the first cyberwar. Jenkinson seems to show favoritism towards the western democratic nation of Ukraine and contempt for the warmongering Russian nation. This resource will be useful for analyzing the affects of contemporary cyberwarfare between Russia and Ukraine in the Russia-Ukraine Conflict.

*Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare* (2022)

Andrew Jenkinson, a U.K. cybersecurity professional with experience as CEO of multiple security companies writes about the various cyberwarfare attack over history. Jenkinson concisely covers the various cyberwarfare between nation-states, such as Stuxnet, SolarWinds, and Sandworm, objectively. Jenkinson gives the context before, during, and after for these various attacks. This resource will be useful for analyzing, with other resources the, affects of these cyberattacks on these nation-states and their societies.

*Cyber Terrorism after STUXNET* (2014)

Thomas M. Chen, a U.K. professor in cyber security describes the events of the Stuxnet attack orchestrated by the United States and Israel, and the aftermath as well as the implications of cyber warfare retaliation and terrorism. Chen summarizes these events objectively and also speaks of how Stuxnet affected the people of the U.S. during the Bush administration, Israel, and Iran. This resource is helpful for determining the affects of the Stuxnet attack on the societies, specifically the people of the U.S. and Israel, and the extremist groups and government of Iran.

*The Stuxnet Computer Worm: Harbinger of Emerging Warfare Capability* (2010)

Paul K. Kerr, John Rollins, and Catherine A. Theohary, researchers for the Congressional Research Service (CRS) writes a full report and summarization of the Stuxnet attack, the results of the attack, the implication on the introduction of cyberwarfare as tactic of espionage and war for future events, and the beginning of a cyber warfare arms race. This resource is made very objectively to summarize the Stuxnet attack to members of Congress and the rest of the United States, but primarily focuses on the implications for the U.S. as well as shows a focus towards United States national security. This report is useful for my project as it shows how the U.S. government began to respond and prepare for cyberwarfare.