2021

Offensive Cyber Operations: An Examination of Their Revolutionary Capabilities

Madelyn Wardle
Wright State University

OFFENSIVE CYBER OPERATIONS: AN EXAMINATION OF THEIR REVOLUTIONARY CAPABILITIES

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts

By

MADELYN WARDLE
B.A., The Ohio State University, 2019

2021
Wright State University

WRIGHT STATE UNIVERSITY

GRADUATE SCHOOL

23 April 2021

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY Madelyn Wardle ENTITLED Offensive Cyber Operations: An Examination of Their Revolutionary Capabilities BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF Master of Arts.

Liam D. Anderson, Ph.D.
Thesis Director

Laura M. Luehrmann, Ph.D.
Director, Master of Arts
Program in International and
Comparative Politics

Committee on Final Examination:

Liam D. Anderson, Ph.D.
School of Public and International Affairs

Carlos E. Costa, Ph.D.
School of Public and International Affairs

Vaughn Shannon, Ph.D.
School of Public and International Affairs

Barry Milligan, Ph.D.
Vice Provost for Academic Affairs
Dean of the Graduate School

Abstract

Wardle, Madelyn. M.A., School of Public and International Affairs, Wright State University, 2021. Offensive Cyber Operations: An Examination of Their Revolutionary Capabilities

Since the cyber realm has become a prevalent area in society, states have been developing ways to use this realm to their advantage. Popular literature asserts that cyber attacks are equalizing, frequently-occurring events that make them “revolutionary” tools of warfare; however, this study hypothesizes that cyber operations are not as revolutionary as the literature asserts. This study examines the revolutionary capabilities of offensive cyber operations by studying documented cases of state-sponsored offensive cyber operations from 2005-2019. By utilizing statistical methods, first the paper examines the documented cases and analyzes which states conduct most of these operations. Then, the paper will use statistical methods to examine the trends in states that have publicly documented instances of cyber operations versus those that do not.

Table of Contents

List of Tables

Acknowledgments

First, I would like to thank my parents and the rest of my family for their support throughout this program, and the rest of my educational career. I could not have done it without your support and encouragement.

I would like to thank my thesis advisor and chair of my committee, Dr. Liam Anderson. Thank you for your support and guidance throughout the process, especially through the beginning and determining the direction of the thesis. Thank you also to Jackie Anderson for her kind words and gesture during a tough time.

I would like to thank Dr. Carlos Costa for all of his help and guidance throughout my degree, helping a political science student understand the world of statistics. Dr. Vaughn Shannon, thank you for being part of my committee and offering helpful advice. To Dr. Luehrmann, thank you so much for all of your support throughout this program.

Finally, I would like to thank my friends and the rest of my cohort for their support and encouragement throughout our time in the program. A special thank you goes to my friend and roommate Kelly Tursic for encouraging me and being there for me, especially through the last year.

Chapter One

Introduction

On December 9, 2020, it was revealed that a top United States cybersecurity firm, FireEye, had experienced a breach, likely perpetrated by a nation-state. Over the next week, it became clear that Russian intelligence agencies had carried out the operation, and it was much more far-reaching than originally realized. The IT management company SolarWinds was the initial target and the path through which the Russian hackers entered these systems, gaining access to United States government networks and potentially thousands of other networks. To this day, the true effects and number of targets are unknown, and investigators may never truly know the full scope of the operation (Barrett, 2020). The following description of events and the scope is the most current information on the offensive cyber operation, however, it is likely that more information will continue to come out as time progresses.

The SolarWinds cyber operation likely began in March 2020, when hackers from one of the Russian intelligence services compromised IT management software from SolarWinds, an IT company. Russia used the hacked program to infiltrate at least 18,000 networks, belonging to a wide range of targets, including both government and private sector targets (Sanger, 2021). The computer security firm FireEye was the first to raise the alarm, when its own networks were penetrated as a result of the operation. The government agencies that have been identified as targets of the operation so far include: the Department of State, the Department of Homeland Security, the National Institutes of

Health, the Pentagon, the Department of the Treasury, the Department of Commerce, and the Department of Energy. To date, it seems that the hackers were only able to gain access to the unclassified systems of these organizations, but the extent of the access and damage is still unclear (Vaughan-Nichols, 2021).

The SolarWinds operation was extremely methodical and was an example of a supply-chain operation. The original intrusion was into a system that SolarWinds uses to put together updates to its Orion product, which is an IT management software that allows organizations to keep an eye on what is happening on their networks. The hackers inserted malicious code into an otherwise innocent software update, infecting the update while it was still under assembly. Instead of trying to trick individuals into downloaded infected malware onto their machines and systems, it packages the malware inside trusted pieces of software. Therefore, the intruders could just rely on private companies and government organizations to install the update with the malware on it at the prompting of SolarWinds, who was not aware that the software was compromised. This operation was carried out very methodically, allowing it to remain undetected for an extended period of time (Hautala, 2021).

One of the most troubling aspects of the operation, besides the direct intrusion onto government networks, was the compromising of the cyber security company, FireEye`s, tools. These tools were used to find vulnerabilities in its clients` systems. Some of these clients included government organizations and intelligence agencies. FireEye uses its tools to conduct benign hacks of its clients` systems in order to discover vulnerabilities and help fix holes in their cyber security systems. Therefore, the hackers now have these tools that FireEye used to discover vulnerabilities, so Russia could now have an advantage and has added these tools to its arsenal (Sanger, 2021). These tools could be used against the United States in the future and will likely be taken into account as vulnerabilities going forward. The implications of this operation are far reaching and will be felt for years to come. This 2020 operation would be the most sophisticated known theft of U.S. government data by Russia since a two-year spree from 2014-2015 (Sanger, 2021).

The SolarWinds operation, and even the hack against the Democratic National Committee in 2016, were far from the beginning of Russia`s offensive cyber operations. In April 2007, riots began breaking out on the streets of Estonia over the moving of a Soviet World War II memorial statue known as the "Bronze Soldier" that the Estonian government was moving from the center of Tallin to a military cemetery outside the city center. Then on 27 April, the first wave of distributed denial-of-service (DDoS) attacks began against Estonian websites. The website of a newspaper, *Postimees*, that usually received about eight to nine thousand comments a day received more than ten thousand comments in ten minutes, which were all a variation of about thirty distinct messages. Within an hour of the attacks beginning, the website began getting 100,000 comments in ten minutes (Sciutto, 2019, pp. 21-25).

These attacks spread out across the private and public sectors, affecting businesses, the media, the financial sector, and government websites and services. They shut down the websites of all government ministries, two major banks, and several major political parties. The parliamentary email server was also temporarily disabled, further complicating the ability of the Estonian government to respond. The attacks were primarily disruptive, affecting the operations of government communication channels and caused interruptions to mobile networks and the emergency services lines. There was a discernable effect for many people because they lost access to services (Haataja, 2017, pp. 160-161) (Herzog, 2011, pp. 50-51).

The Estonian population was one of the most connected in the world at that time, which left them more vulnerable than other states would have been. The DDoS assaults cut off the access of Estonians from their news and government websites, making it difficult to impossible for citizens to know what was happening. These disruptions seriously impaired the daily operations of many organizations from small to large, including banks, government departments, and small businesses. Estonian society was very dependent on the internet and other technology, due to their structure. The economic effect of these attacks has been estimated to be anywhere from 27 to 40 million U.S. dollars, demonstrating a large effect (Haataja, 2017, pp. 160-161). The attacks have been attributed to Russia, but only a single Estonian citizen was charged, and Estonia could not retaliate, and struggled to deal with the attacks when they were happening (Sciutto, 2019, pp. 23-25). These attacks demonstrated the potential damage that another country could do to another only utilizing cyber tactics.

Over the last twenty years, as people, industries, and states have become dependent on the cyber space, states and other groups have used this dependence to their advantage. They have exploited others through cyber space by many techniques, including data destruction, defacement, denial of service, doxing, espionage, financial theft, and sabotage (Council on Foreign Relations, 2020). The attacks against Estonia demonstrated that large/strong states can use cyber operations against smaller/weaker states, but cyber operations can be used by smaller/weaker states against larger/stronger states as well. According to Sethi, “It`s difficult to name a country that does not perpetrate cyber crimes these days to spy on countries and cement its political influence” (Sethi, 2020, 196-197). While this statement may be true, it is difficult to say that all of the techniques listed above should be considered an act of aggression. It especially could not be said that all of these techniques could be considered a form or instigation of “cyber war”.

Another aggressive form of cyber tactics is espionage, which can be used for economic, technological, political, or military gain. China frequently uses espionage as a tool against its opponents, including the United States. In July 2015, it was discovered that Chinese hackers had targeted and successfully penetrated the United States government`s Office of Personnel Management. Through these operations, China gained access to the security clearance information of tens of thousands of United States government employees. This data contained potentially damaging personal information and could have been used to exploit government employees to the advantage of the Chinese government. It was unclear what information was stolen or accessed, which almost increases the potential for damage because it is unclear what China might be planning to do with the data (Schmidt, 2015).

Iran has conducted many documented state-sponsored cyber operations on a variety of targets from at least 2010 until the present. This has included several against strong states, such as the United States. In 2019, Microsoft announced that hackers linked to the Iranian government tried to infiltrate the email accounts of a U.S. presidential campaign, current and former U.S. officials and journalists, and others (Sebenius, 2019). Over an approximately thirty-day period between August and September, the hackers "made more than 2,700 attempts to identify consumer email accounts belonging to specific Microsoft customers and then attack 241 of these accounts" (Sebenius, 2019).

Microsoft did not officially announce which presidential campaign was targeted, but inside sources told the New York Times that the campaign was President Trump`s. This attack took place after the Trump administration announced additional sanctions against Iran following the withdrawal of the United States from the 2015 nuclear deal with Iran. These sanctions were intended to choke off the country`s oil revenue, and Iranian officials have admitted that these sanctions helped plunge the Iranian economy into a recession (Perlroth and Sanger, 2019). While it is unclear if the cyber operations against presidential campaigns were a direct result of the increased sanctions, it is possible that they were Iran`s attempt to respond. According the *New York Times*:

> "The surge has led American officials to a stark conclusion: For Iran, cyberespionage — with the power it gives the Iranians to jab at the United States and its neighbors without provoking a military response — is becoming a tool to seek the kind of influence that some hard-liners in Iran may have hoped its nuclear program would eventually provide. While American officials doubt cyber skills, or even the most advanced cyber weapons, will ever have that kind of power, Iran's cyber focus these days is notable" (Sanger and Perlroth, 2015).

This analysis was written in 2015, after it was discovered that Iranian hackers had targeted the State Department of the United States.

In 2014, Sony Pictures was getting ready to release a new comedy, *The Interview*, whose plot revolved around two actors trying to assassinate North Korean leader Kim

Jong-un. North Korea warned Sony not to release the film, and when Sony refused to comply, North Korean agents hacked Sony. The hackers compromised at least 100 terabytes of data and released personal and confidential information online, including email chains between executives. Sony eventually cancelled the release of the movie in theaters but released it on online streaming services (Sethi, 2020, 160-182). This was a state-sponsored operation against a private entity within another state that demonstrated how states are affected by and will respond to offensive operations that target entities within their borders.

States across a wide spectrum of military power, economic power, and levels of democracy have conducted offensive cyber operations. These operations have been against a wide range of other states, including both weaker states and stronger states relative to the aggressor state. Have cyber tactics allowed weaker states to conduct offensive operations against stronger states, and changed the balance of power in conflict? In some cases, these tactics have been integrated into warfare, but are they integral to modern warfare? Moreover, many states are capable of carrying out these operations, but relatively few have been publicly documented as carrying out offensive cyber operations, even less that qualify as actual “cyber attacks”, and none have been documented conducting “cyber war”. The following chapters will attempt to answer these questions and establish patterns to be able predict state behavior in the future.

Chapter Two

Cyber Attacks: A Revolutionary Weapon of War?

In 2013, the chief of staff of Russia`s military, General Gerasimov, commented on the potential effectiveness of “unconventional modes of warfare”: “The very ‘rules of war’ have changed,” he wrote. “The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power . . . of weapons in their effectiveness.”” (Sciutto, 2019, p. 13). Cyber operations have clearly played a role in changing the rules of war, however, it has yet to be determined just how effective they are. This paper will focus on state actors, because although non-state actors act in the cyber realm, the most sophisticated capabilities still belong to states (Buchanan, 2016, p. 11).

Defining “Cyber”

The terms “cyber” and “cyberspace” have never been given a precise definition on which experts and societies have reached a consensus. Many authors do not begin their books or articles by defining the definition of cyber and cyberspace that they are using. Publications about offensive cyber operations, including cyber wars and cyber attacks, discuss the definitions of the terminology, though it would likely be more helpful to break it down to the more basic level of defining cyber in order to ensure real understanding of the terms. This implies that there is one set definition of the term “cyber attack”, not necessarily even in just the expert community, but in the general world as well, because materials intended for the general public do not discuss defining the term explicitly either. This could lead to misconceptions about the realities of cyberspace and its related issues, so the starting point for current purposes is a discussion of various definitions of the term and a clear explanation of the definition to be used.

The book *Cybersecurity and Cyberwar: What Everyone Needs to Know* by Singer and Friedman is a foundational book on cybersecurity, that is written to be accessible for people who do not work in the cyber field. They recognize and discuss that the definition of cyber or cyberspace is complicated and stick with a simple definition for the purposes of the book. They define cyberspace as the "realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online" (Singer and Friedman, 2014, pp. 13). They also acknowledge that the cyberspace is not completely virtual and involves the systems and infrastructures that allow it to work. Clarke and Knake break it down even more simply, saying that cyberspace is simply all of the computer networks in the world and everything they connect and control (Clarke and Knake, 2010, pp. 70). These definitions are very straightforward and allow a broad spectrum of things to fall under the umbrella of "cyber" and "cyberspace".

Scholarly analyses intended for audiences already familiar with cyber issues, are less likely to define "cyber", but some do address the issue at a more complex level. For example, Choucri and Clark (2018, p.3) state:

> "In this book we view cyberspace as a global domain of human interaction that (1) is created through the interconnections of billions of computers by a global network, today the Internet; (2) is built as a layered construct where physical elements enable a logical framework of interconnection; (3) permits the processing, manipulation, exploitation, augmentation of information, and the

> interaction of people and information; (4) is enabled by institutional intermediation and organization; and (5) is characterized by decentralization and interplay among actors, constituencies, and interests."

This definition is much more specific than the first two examples but covers the same basic ideas. Cyberspace has both physical and virtual components, that much is clear from all of the definitions, both simplistic and complex. Cyberspace can involve the internet, networks, and the physical systems infrastructure, that is clear from every definition. This definition also makes the interplay among actors clear, which is an important aspect for the current purpose. Therefore, the Choucri and Clark definition of cyberspace will be used here, due to its comprehensive nature and specificity beyond the very basic terms.

Defining Cyber Attacks

The popular literature in the field of cyber security asserts that cyber attacks are a revolutionary tool for smaller/weaker states that will give them a level of equal power to stronger states (Buchanan, 2020; Scuitto, 2019). However, not every offensive cyber operation qualifies as a cyber attack in technical terms. Many scholars define every operation as a cyber attack, but this is not the position of this paper. This section will define cyber attacks to demonstrate what is discussed in scholarly literature, but this paper will use the terminology "offensive cyber operations." To begin, there must be a solid definition of cyber attacks. According to McGavran, "Some 120 nations are using the Internet to help fulfill their own "political, military, economic espionage" goals" (McGavran, 2009, p. 260). McGavran`s article was written in 2009, so these numbers have increased even more since then. The very term “cyber attack” is amorphous and is used to describe everything from espionage to denial of service attacks, ranging from attacks that are merely annoying to those that could have catastrophic consequences (McGavran, 2009, p. 261). People use the term “cyber attack” to group all different types of Internet-based attacks together, which can make the perception of the threat more dangerous because states cannot address all cyber attacks in the same manner, and they do not all have the same effect. As stated by Friedman and Singer, “Essentially, what people too often do when discussing “cyberattacks” is bundle together a variety of like and unlike activities, simply because they involve Internet-related technology” (Friedman and Singer, 2014, p. 68).

There are many possible definitions of the term “cyber attack”. Friedman and Singer do not provide a concrete definition but offer advice on how to recognize them. They say that there are two ways to define what a cyber attack is. First, it must be distinguished from traditional attacks, using a digital means or computer. This means that a cyber attack is not constrained by the typical limits of traditional attacks. A cyber attack can also be attacking multiple targets at one time. Second, a cyber attack differs from a traditional attack due to its target(s). A cyber attack always targets another computer and the information in it first. Even if the intended damage is physical, the attack will always originate in the digital world (Friedman and Singer, 2014, pp. 68-69). McGavran argues that “focusing on the primary intent of the cyber attacker is a workable way to deal with interpretive problems posed by cyber attacks” (McGavran, 2009, p. 261). Due to the theoretically low amount of resources needed to carry out a cyber attack, it could make advanced cyber capabilities more possible for states that are typically seen as smaller or weaker.

For the purposes of this analysis, the definition of cyberspace includes both the virtual world, and the physical aspects that control and support it, therefore, a cyber attack should be anything that attacks these components. However, the distinction made by Friedman and Singer that the attacks need to target another computer and the information in it, is an important one. Typically cyber attacks are virtually-based, however some (such as Stuxnet, which will be discussed later), target the physical computer system itself in order to manipulate the information within it. All attacks that target computer systems and the information in them virtually and physically will be included in this study.

Characterizing Types of Offensive Cyber Operations

As discussed, people use the term “cyber attack” to group all different types on Internet-based operations together, which can make the threat more dangerous because states cannot address all cyber operations in the same manner and they do not all have the same effect. As stated by Friedman and Singer, “Essentially, what people too often do when discussing “cyber attacks” is bundle together a variety of like and unlike activities, simply because they involve Internet-related technology” (Friedman and Singer, 2014, p. 68). One of the first steps and keys to studying cyber issues and how they can be utilized is defining some of the major concepts: cyber attack, cyber war, and cyber espionage. The concept of cyber attacks was discussed in the section above, and will be explained further here and in the following sections. Cyber war and cyber espionage will be explained in this section and the following sections.

Cyber attacks can also be distinguished from one another by using the three factors that are known as the CIA triad: confidentiality, integrity, and accessibility, in order to assess the goals of the attacks. For some, "the best way to categorize attacks is by which of these three goals is being threatened" (Friedman and Singer, 2014, p. 70). Confidentiality attacks involve attempts to gain access to the system in order to monitor and gain access to the information on the systems and the users. Integrity attacks are efforts to compromise and change the information in the system, not to remove it. Accessibility attacks prevent access to networks, such as with denial of service attacks (Friedman and Singer, 2014, pp. 70-71). All of these can be destructive, but they each have distinct effects, so they need to be analyzed differently. In addition, all three types of attacks help erode the faith of the public in cyber systems, causing more damage.

One type of cyber operation is cyber espionage, which falls under the confidentiality part of the triad. It attempts to gain access to confidential information using the internet. Cyber espionage is not just something that is done against states, but it can be done against individuals as well. However, it is most commonly done against states, industries, and government agencies. This is a unique form of espionage because the perpetrator does not have to be within the borders of the country to carry it out, limiting the legal authority that the targeted country has over the perpetrator even more. Cyber espionage can also be done for economic reasons, attempting to gain an economic edge. (Friedman and Singer, 2014, pp. 91-96; McGavran, 2009, p. 262). As Friedman and Singer state "Cyber espionage is turning into a major political problem more due to the accusations of intellectual property (IP) theft than political secret theft" (Friedman and Singer, 2014, p. 95). Perpetrators of cyber espionage are even harder to catch because they do not have to be in the country in order to carry out the attack, making it harder to catch and charge a physical person with espionage.

Denial-of-service (DoS) and distributed-denial-of-service (DDoS) operations are forms of accessibility-based cyber operations. These attacks attempt to bring down a website or service center by sending it too many data requests at once, so that the site cannot respond to legitimate requests. These attacks hijack computers that were already infected with a virus that allows hackers to control them. Hackers can control millions of computers at one time for very little financial cost, increasing the effectiveness of their attacks (McGavran, 2009, p. 262). North Korea launched denial-of-service attacks against the United States in 2009 that affected anywhere from 60,000 to 160,000 computers, using them to shut down various government agency and financial websites. Most of the computers used were not located in North Korea, and many of the hijacked computers were actually located with the United States (Kaplan, 2016, p. 213).

Two other types of cyber operations are called "logic bombs" and "Trojan horses" A logic bomb does not affect the computer immediately, allowing it to spread to more and to more devices before it is discovered. It does not activate until certain conditions are met, then it becomes malicious. Trojan horse software tricks a computer into thinking that it is harmless but gives control to a third party that can make it a botnet and take control of the device. A Trojan horse was used by the Israeli government in 2007 to infiltrate Syrian computers, penetrating them to examine Syrian air defenses. They did not activate the virus until they were ready to put false images on the air defense monitors to cover up their fighter planes flying into Syrian airspace to attack a Syrian target, the Syrian military had no idea what was happening. This demonstrated how effective this form of operation could be (Friedman and Singer, 2014, pp. 124-127; McGavran, 2009, p. 263).

A popular form of cyber operation that is used to target both state actors and individuals is phishing. Phishing attempts are generally conducted by emails that are sent to try to get the recipient to click on something that downloads a virus to their device or allow the attacker to gain access. Spear-phishing is a more targeted form of phishing, generally using a form of social engineering to cater the email to the specific target to make them more likely to click on it. This technique has proven so effective that about two-thirds of cyber espionage operations use it. Whaling is a technique that targets a high-ranking individual, such as the CEO of a company or a high-level government official (Buchanan, 2016, pp. 37-38).

Zero-day vulnerabilities are a huge concern for companies and governments. They are vulnerabilities that the company or government does not know about until they are exploited. Most will not even realize they are being targeted until the attack happens. As hard as they might try, companies and governments will never be able to find all of the possible vulnerabilities, they just need to prepare as best they can and realize the risks. There are some individuals and companies who work to find these vulnerabilities and sell them, either to the companies themselves or to attackers (Harris, 2014, pp. 100-104).

Cyber War

There is a significant amount of debate about what qualifies as cyber war. For Clarke and Knake (2010, p.6), cyber war comprises “actions by a nation-state to penetrate another nation`s computers or networks for the purposes of causing damage or disruption.” Burton (2015, p.301), meanwhile, argues that it is the political nature of cyber attacks that qualifies them as warfare. He also adds that since states have been using cyber operations to aid military attacks and have militarized their capabilities, those cyber operations count as cyber warfare (Ibid). By 2010, according to Clarke and Knake some twenty or thirty states had already developed offensive cyber units, and that number has grown exponentially since then (Clarke and Knake, 2010, p. 46).

Another perspective of the debate is that the term “cyber war” is conflated and misnamed. Echevarria argues “What is commonly, and rather loosely, referred to as cyber war is really a three-way competition between the rapid migration of essential data and functions to online networks, which creates very attractive targets; the ongoing efforts of cybersecurity systems, which struggle to protect those networks; and the persistent attempts of cyber attackers, whether criminals or spies, who find ways to defeat those security measures” (Echevarria II, 2017, p. 100). He also brings up the point that since there are often no casualties and no physical damage, some people believe that it cannot qualify as war (Echevarria II, 2017, p. 99). These points have merit. However, most states view cyber tactics as a form of warfare and treat them as such, therefore they should be considered in that light.

Some RAND analysts defined cyber war as “any means of warfare that shifts the balance of knowledge in the attacker`s favor (Greenberg, 2019, p. 77). Author Andy

Greenberg emphasized a quote from a cyber security fellow at the Atlantic Council: “The physics of cyberspace are wholly different from every other war domain” (Greenberg, 2019, p. 217). This highlights one of the most challenging aspects of dealing with cyber warfare, which is that the lack of conformation to the physics of conventional warfare indicates that the problem needs to be dealt with in a different way. Leaders and experts from around the world have yet to agree on definitions of cyber attacks and cyber warfare, which must be done before policies and responses can be formulated. Some states have chosen to take advantage of this lack of a unified response from the world community and the anonymity that can often accompany cyber warfare.

One of the biggest challenges in combatting and dealing with cyber warfare is the difficulty of concretely attributing the attacks to a state, referred to by many in the community as the “attribution problem”. While sometimes the attacks can be traced back to the “command and control” servers that controlled the attack, their location in a certain country does not automatically confirm that the attack was state-sponsored. World leaders often want to know who committed the attack in order for retribution, but this is often not possible. States often deny their involvement in cyber attacks even when attacks can be concretely traced back to them, making the problem more difficult. However, when states claim responsibility for cyber attacks, it signals their seriousness about the issue at hand (Clarke, 2010, pp. 25, 213-215). The attribution problem makes it difficult for states to retaliate, either in the cyber realm or militarily, or with other methods such as diplomatic or economic sanctions.

Clarke and Knake explain some of the dilemmas experienced by states when it comes to cyber warfare. They discuss the need to act first because of the pace that conflicts move in cyberspace. Strategy dictates that if a state does not act quickly or first, they might not be able to act at all. The states that attack first can disable or significantly weaken the ability of the state they are attacking to strike back. However, most of the existing literature on strategy in cyber conflicts does not discuss the potential disadvantages associated with striking first (Clarke and Knake, 2010, p. 45). These are just a few of the problems states face associated with cyberspace.

This paper will not be looking at the issue of cyber warfare in depth, but acknowledges that the concept of cyber warfare is important in modern warfare and international relations. Offensive cyber operations and cyber attacks are a component of cyber warfare, however this study will be looking at offensive cyber operations on more of an individual operation basis, as opposed to looking at or for an overarching campaign of coordinated attacks.

Defining “Revolutionary”

The term “revolutionary” can have many different meanings and connotations to different people. In the United States, people often think of the Revolutionary War and relate it to that. Merriam-Webster`s dictionary defines revolutionary as “constituting or bringing about a major change”, and relates it back to the term revolution, which it defines as “a sudden, radical, or complete change” (Merriam-Webster, n.d.). This idea of a major change is central to this paper.

In order for something to be considered revolutionary, it needs to bring about a major change, a shift in the way things are done. This paper will focus on the concept of revolutionary in terms of tools of warfare, as will be discussed in the next section. The potential revolutionary tool that will be discussed is the cyber realm, looking at how cyberspace and cyber offensive cyber operations have or have not brought about change.

Revolutionary Military Technologies

This potential ability of weaker states to obtain an advanced capability to rival that of stronger states could make offensive cyber operations (or cyber capabilities in general) a revolution in military affairs. A revolutionary military technology is one that changes the face of warfare and gives new advantages. As Davis explains, "revolutions are not merely more clever technology" and they involve "dramatic breaks with the existing status quo" (Davis, 1996, p. 44). This supports the idea that revolutionary military technology must change the face of warfare while also changing the status quo. Davis also states that when it comes to revolutionary military innovation:

> "Technology alone is not sufficient to produce a military revolution; how military organizations adapt and shape new technology, military systems, and operational concepts is much more important." (Davis, 1996, 47)

In order to change the status quo, the revolutionary technology must give power to states that did not have as much power before.

There have been several revolutionary military technologies that have developed over time, such as handguns, submarines, and nuclear weapons. Handguns were a revolutionary technology because before their development, people had to be able to physically beat their opponent through strength. With handguns, weak people were able to defeat stronger people because guns do not require the user to be stronger. Submarines were revolutionary because they allowed military forces to move through the water virtually undetected and made it more difficult for navies to attack each other. Nuclear weapons were revolutionary because of their ability to kill large numbers of people and cause widespread destruction with a single bomb/missile. This would give any state that possessed these capabilities an advantage, no matter the size of the state.

Based on these examples, a technology should only be qualified as revolutionary after it meets several qualifications. In all of the examples, the use of that technology increased exponentially over time. Handguns spread throughout the world, and they are very easy to find today. They have given weak actors an advantage over strong actors for over a century. Submarines have become a common tool for any state with a naval force, giving them the ability to move covertly. Nuclear weapons are highly coveted throughout the world, and many countries are trying to develop that capability. Nuclear weapons have also brought a new factor/level of deterrence that is considered in worldwide conflict. They give any state that has them, no matter how weak, a bargaining tool. They also add a certain level of protection for those states because other states are much less likely to attack a state conventionally or with nuclear weapons if the state begin attacked possesses nuclear weapons. Cyber tactics have spread through parts of the world, but they are not as widespread as experts claim they should be. Some scholars claim that these tactics could be used by any state with a computer, however this has not been seen in practice.

Scholars argue that cyber capabilities could be an equalizing factor between weak and strong states and offers a new realm of strategy for states. Unlike nuclear capabilities, cyber capabilities could potentially provide substantial regime security at a fraction of the cost (Rustici, 2011, p. 36). The difference in cost makes cyber capabilities more accessible and widespread, which adds to its revolutionary potential. This leads scholars to compare cyber capabilities to nuclear capabilities, a revolutionary tool of warfare (Ibid; Sharma, 2010).

While cyber and nuclear are very different technologies, it can be useful to compare them in terms of their revolutionary potential. Sharma discusses this phenomenon in a 2010 paper, explaining why cyber tactics should be considered a revolution in military affairs. He argues that cyber tactics have the same strategic effect as other revolutions in military affairs, such as artillery and nuclear weapons, in that they have had a large strategic effect and have had an impact in creating a new world order (Sharma, 2010, pp. 63-64). The effects of cyber warfare are potentially like nuclear warfare, in that they can be far-reaching, devastating, and unmeasurable (Sharma, 2010, p. 70). However, these capabilities have never been truly proven.

Cyber theory has had some of the same struggles as early nuclear theory as well. Due to the lack of true cyber warfare events (and therefore, case studies), there is uncertainty about what the potential destruction and effects could be (Rustici, 2011, p. 34). This ambiguity also lends to its revolutionary capability, because it has a strong psychological effect of fear, as some have called it a “weapon of mass psychological destruction” (Sethi, 2020, p. 5). While it may or may not turn out to be a weapon of mass destruction in the traditional sense (physical destruction caused), the lack of warning associated with cyber operations can add to the damage they cause (Rustici, 2011, p. 40).

The uncertainty about the destructive capabilities of cyber operations means that they might not have truly revolutionary effects.

Other scholars argue that cyber operations are not a completely revolutionary tool. Valeriano, *et al.* argues that cyber campaigns are not as revolutionary or effective as people claim when the evidence is evaluated (Valeriano, et al., 2018, p. 2). They argue that "Cyber operations complement rather than replace traditional statecraft. We find that cyber means serve as an additive foreign policy tool in modern strategic competition" (Valeriano, et al., 2018, p. 3). This could be supported by the assertions of other scholars that cyber operations are supplementary tools of statecraft, not methods that can stand on their own.

Other scholars have argued that while cyber tactics might not be revolutionary, they can be used as a force multiplier or coercive tool along with other methods. Cyber capabilities have limited effectiveness as an independent tool of coercion and are only part of a state`s "coercive toolkit" (Borghard and Lonergan, 2017, p. 453; Poznansky and Perkoski, 2018, p. 402). However, not all cyber operations are attempts at coercion, though they can have second-order effects of escalation in foreign policy (Whyte, 2020, p. 213). Based on the current cyber capabilities of states, attrition, denial, and decapitation strategies are the most likely to be effective in the cyber realm (Borghard and Lonergan, 2017, p. 454).

Cyber Use By Economically Disadvantaged States

Economically and technologically disadvantaged states still desire to have cyber capabilities and have attempted to advance with the rest of the world, despite economic status. As Kshetri states:

> "Some analysts predicted that technologically backward states may face greater challenges and difficulties to fight a cyber-war. Yet contrary to these stereotypes, so called "rogue" and economically backward regimes have not been passive observers of cyber-attacks and cyber-warfare. Indeed, quite the opposite, some such nations have advanced cyber-warfare capabilities and potential to inflict harm and damage to their adversaries" (Kshetri, 2016, p. 6).

In other words, many smaller states have realized the potential opportunities that lie in the cyber realm, and how they can use them to their advantage, since they might not be able to compete in conventional military terms. Cyber weapons have a wide range of applications while also being exceedingly cheap, making the available destructive capacity for weaker states "unprecedented" (Rustici, 2011, p. 34).

Scholars, especially in popular literature, argue both for and against the idea that cyber operations will give weaker states the ability to attack stronger states. In some cases, cyber warfare is referred to as hybrid warfare, and scholars have suggested that in a world with one superpower, the rise of this type of capability was inevitable so that declining and rising powers can challenge the single superpower (Sciutto, 2019, p. 16). While these capabilities may have begun with stronger states, cyber capabilities spread from great powers to weaker states (Buchanan, 2020, p. 316).

> "Cyber is a tailor-made instrument of power for North Korea. There`s a low cost of entry, it`s largely asymmetrical, there`s some degree of anonymity and stealth in its use. It can hold large swaths of nation-state infrastructure and private-sector infrastructure at risk. It`s a source of income." (Sethi, 2020, p. 163)

Sethi utilizes this quote from a National Security Agency official, which seems to support the argument that cyber capabilities give weaker states an advantage. But it also emphasizes the economic aspect of it for weaker states, which does not necessarily aid its military power.

Cyber Strategy/Doctrine

Cyber tactics and doctrine hold promise for grand strategy in the opinion of military and academic strategists. Some believe that a cyber war attack response should include deterrence measures and escalation levels, with some, such as Colarik, comparing it to the response that states would have to a conventional attack. This includes attempting to make sure that opponents cannot form an opposition by impeding their supply networks and means of communication. They assert that proportionality is still key in responses to cyber operations in order to maintain the high ground and ensure that the state`s strategic goals fit within a proportional response (Colarik and Janczewski, 2011, pp. 54-55). This idea of keeping the response to cyber operations proportionate to the original attack brings up the question of what qualifies in that sense. If a cyber operation is particularly destabilizing or overarching, does the target state have the right to respond with conventional tactics? The answer to this question is outside the scope of this paper, however the question is important to consider when thinking about why or why not states choose to carry out offensive cyber operations.

The early detection of cyber operations is crucial to combatting them and can limit their damage. It can be difficult to go on a counteroffensive against the attackers to strike back in self-defense (Osawa, 2017, p. 127). Osawa, for example, examines recent cyber operations involving states from approximately 2007-2017, which show that cyber operations typically follow incidents of international discord and/or conflict (Osawa, 2017, p. 113). This demonstrates that states use cyber operations as a strategy to deal with international conflict aggressively, but without using conventional weapons. This can communicate their message without firing an actual shot. Cyber methods can be used in many ways related to warfare, including as cyber warfare itself, and this paper will examine what drives states to use these methods.

Cyber Deterrence

There are many debates about the role of cyber operations in deterrence. However, many scholars who argue that deterrence is difficult in the cyber realm do not take into account that cyber operations are ultimately inseparable from the physical domain. This gives cyber operations more geopolitical context and physical context, where deterrence has proven effective time after time (Goodman, Will, 2010, p. 102). According to Goodman, in order to have an effective cyber deterrent a state "must have at least geopolitical symmetry with its adversary, if not a favorable asymmetry, to protect itself as the conflict in cyberspace escalates and spills over into the physical domain" (Goodman, Will, 2010, p. 109).

This idea demonstrates that the cyber domain does not and cannot operate in a vacuum separate from geopolitical factors in the physical world, one must impact the other. An issue with deterrence being effective in the cyber realm is the attribution problem, so in order for cyber deterrence to work, states must clearly communicate their intentions and actions to other states in order for their actions in the cyber realm to be considered deterrence. It would also be helpful for states to make their "red lines" clear, in order for other states to know how to deter them effectively, knowing what lines are acceptable to cross without prompting a conventional response (Goodman, Will, 2010, p. 129).

Cybersecurity Dilemma

The security dilemma is a long-standing idea and theory of international relations, promoted by Robert Jervis (Jervis, 1978, p. 170). The basis of it is that as states secure themselves, they inadvertently cause fear in other states (Buchanan, 2016, p. 3). This can be said for many aspects of security, including building up conventional forces, creating a missile defense system, and developing new technologies to increase the state`s advantage in warfare. Cybersecurity and cyber tactics have not escaped this dilemma.

The cybersecurity dilemma can help explain the fear caused by network intrusions between states. With conventional attacks, it is very obvious when states are preparing for an attack, and the attacking state can expect a fight once it crosses the physical borders of another state. However, with cyber operations, offensive forces can make their way into the systems of another state undetected and the defending state is often unsure if it will be able to fight off the offensive (Buchanan, 2016, pp. 4-5). The idea of zero-day vulnerabilities come into play here, because unlike with conventional, physical buildup, a state does not know its vulnerabilities until they are exploited. This could cause any network intrusion to be seen as very aggressive and potentially destabilizing.

States can choose to invest in either intrusion or security capabilities, or both, but not all states choose to invest in both. Their choice to invest in one instead of the other or one more than the other can be perceived in many different ways by other states. As with traditional, conventional methods, cybersecurity methods intended to be defensive can also be perceived as offensive, and the buildup of cyber defenses can be seen as anticipating an imminent conflict. It can also be difficult to distinguish between states infiltrating the networks of other states for espionage purposes or more attack/offensive purposes, such as data destruction and military purposes. This could make states less likely to engage in cyber action of any kind (Buchanan, 2016, pp. 188-189).

Economic Factors

The role of economics in this paper is to determine whether the level of economic stability/success has a role in whether or not a state decides to utilize cyber warfare. This paper recognizes that economics plays a crucial role in all areas of world affairs. While cyber warfare is often seen as more cost-effective and low-cost, it is not immune from economic constraints. Both the attacker and the target have the potential to suffer economic consequences. Sometimes the intent of the attacker is to exact purely economic consequences on the target. Network intrusions and intellectual property theft can cause very real economic damage to companies, governments, and countries as a whole. However, these types of attacks are generally not viewed to be enough to warrant a full-scale response, especially not militarily. As Buchanan discusses, retaliatory economic sanctions could be used, but they are often not effective tools, especially to combat cyber actions (Buchanan, 2016, pp. 91, 184-185).

Countries with developing economies are more likely to suffer as a result of cyber operations related to cyber crimes as opposed to more developed countries. They are also likely to have citizens committing cyber crimes as well. These are often committed by non-state actors such as organized crime organizations or terrorist groups, who often exist in states who are cyber actors as well (Kshetri, 2010, p. 1057). However, the focus on economics of this paper is on the point at which the state will engage in cyber warfare, not how it is economically vulnerable or when it will resort to cyber crimes.

Military Factors

The importance of size and firepower for military might is obvious and has withstood the test of time. With the development of cyber techniques, how the world defines the strength of a state could be changing. However, it should be studied if military strength is still a factor in whether or not states decide to engage in offensive cyber operations. There have also been military branches developed for both offensive and defensive purposes by governments around the world in order to engage with other states in the cyber realm, such as Cyber Command in the United States (Clarke and Knake, 2010, p. 46).

There is debate as to the relationship between war and the growth of technical industries, and this could likely be said for the relationship between technical industries and cyber warfare as well. Ruttan discusses the idea within the context of the United States that without the drive for military procurement, certain sectors may not develop as quickly or robustly (Ruttan, 2006, p. 160). Due to the fact that societies are so dependent on technology it is likely that the cyber industry would develop regardless. However, the cyber warfare capabilities would likely not develop as well if there was not a militaristic functionality. States will continue to develop their cyber warfare capabilities as long as that potential is there.

Military experts agree that any war from now into the future will involve the use of cyber power. However, they disagree about the point at which cyber aggression becomes cyber war. Echevarria II says "We may define cyber power as the ability to operate with relative security within cyberspace; cyber war or cyber warfare, in contrast, generally means using digital "code" to inflict material or psychological harm on another party, and thereby to coerce that party into doing what we want" (Echevarria II, 2017, p. 99). This distinction is important in order to understand how states will use these tactics either separately or in conjunction with their military tactics.

Since the development of the first nuclear weapon in the 1940s, states have coveted and closely guarded their nuclear arsenals. Nuclear weapons will always play a factor in world affairs and military strategy, and this paper will study if the possession or lack of nuclear weapons plays a role in whether states will decide to use cyber operations or cyber warfare. States fear that their arsenals are less secure now and that their weapons and facilities are susceptible to cyber operations. States have done tests to determine their vulnerabilities and have worked to fix them, but there will always be work to do (Harris, 2014, p. 140).

Valeriano and Maness Study

Valeriano and Maness created a comprehensive data set that demonstrates that cyber tactics are not as revolutionary as some scholars claim. They organized their data set by dyads, and for each overall incident within a dyad they expanded the data along many factors, including target type, severity, and damage type. One of the key factors of the data set is the damage type section. They ranked the damage caused by cyber attacks/cyber operations on a scale of 1-10 by type and severity of damage. This demonstrated the lack of revolutionary cases to date because none of the cases had damage scores larger than 4. Therefore, while cyber tactics can be used as acts of aggression between states, they do not cause a large amount of damage, which is relevant to any assessment of the revolutionary potential of cyber war (Valeriano and Maness, 2020).

Conclusion

Even though cyberspace has existed for public use for over two decades, there are still significant knowledge gaps in its use and how it will grow in the future. As the data set and evidence will show, state-sponsored offensive cyber operations have been occurring since at least 2005 (that the public is aware of), but there is still very little concrete knowledge about how they will be employed and the difficulty (or ease) of using them. All of the components discussed (cyber space, offensive cyber operations, revolutionary military technology, cyber strategy, etc.) are integral to this study, and how they will be integrated and used will be explained in more detail in the next chapter.

Chapter Three

Code Book

Purpose

This study examines whether offensive cyber operations are truly revolutionary tools of warfare, or if they are simply a new technology, whose true level of utility is still being realized. As discussed in the literature review, there is significant debate among scholars in all areas concerning cyber, including whether or not it is a revolutionary capability. Literature more designed for the masses, and non-practitioners in the field, seems to overwhelmingly say that cyber operations are revolutionary tactics. However, they do not necessarily offer more than anecdotal evidence and select cases to back up these claims. This study analyzes different factors in two separate data sets to examine the trends and offer more solid evidence for whether or not cyber operations are a revolutionary military technology for states.

The purpose of this paper is to add to existing research on offensive cyber operations, and which states choose to use them. The following section will use measures of state strength to compare the states that are cyber aggressors to the states that are targets of their cyber operations and the states that choose not to carry out cyber operations. This will help determine if offensive cyber operations are a revolutionary tool because if there are more stronger states conducting offensive cyber operations against weaker states than weaker states against stronger states, then cyber methods might not be as revolutionary as some of the literature asserts. Determining which states choose to utilize cyber operations and which states choose not to will also help demonstrate whether they are revolutionary tools, because a truly revolutionary tool will be used by states with a wide variety of levels of power.

In the Revolutionary Index Data Set, whether or not offensive cyber operations are revolutionary will be determined by if there are more instances of weaker states attacking stronger states, showing that cyber operations are an equalizing tool. This would demonstrate that cyber operations allow weaker states to contend with stronger states, which could help demonstrate that it is revolutionary if that occurs more frequently than simply stronger states using it as another tool to control weaker states.

In the Revolutionary Capability Data Set, whether or not offensive cyber operations are revolutionary will be determined by looking at the states that choose to carry out cyber operations versus the states that do not. The metrics will help determine if there are certain factors or certain levels of power (economic, military, etc) at which states decide to carry out offensive cyber operations.

Scope and Limitations

There are a large number of cases of cyber operations perpetrated by and against states, against individuals, groups, and states. There are hundreds of documented cases of cyber operations that are public knowledge. It is important to recognize, however that there are likely many more cases that the public is not aware of that could either support the paper or give evidence against it. This is an accepted limitation of the paper, as states do not want to admit their vulnerabilities, so this is unavoidable. There have also likely been many more attempts by states to conduct cyber operations against other states that have not been successful, and were therefore not reported. If these attempts were successful enough to be caught and recorded, they are included. However, there are many attacks that do not make it past defenses and basic system security, that states and entities do not have to deal with more in depth, since their systems catch them first.

Beyond merely the limitation of publicly available information about cyber operations, the cases included in this paper might not be an exhaustive list of state-sponsored cyber operations that are public knowledge. The cases of offensive cyber operations that occurred were based on a specific source, and different organizations have conflicting information. This paper uses a single, specific data source – the Council on Foreign Relations Cyber Operations Tracker dataset – to limit the need to mediate between datasets and accepts the limitations of sticking to that data set.

The dataset includes cases of state sponsored cyber operations against other states, or entities within states. Cyber operations perpetrated by independent groups (not affiliated with governments) or individuals, are outside the scope of this paper. Independent groups are not constrained by the same factors as states; however, they also do not necessarily have the power that states have either.

State power, especially relative state power, is very difficult to measure with precision. Metrics based on a per capita measurement can be deceiving when it comes to states that have large populations, such as China and India. Based on GDP per capita, countries with large populations will rank lower, even if they are actually rich states with vast resources, such as China. This could end up showing that Saudi Arabia or Sweden are more powerful than China, which most people would agree is not accurate, however that is what the measure shows. This is an issue with all per capita measures, such as military expenditure as well. That is why there are multiple different metrics being used and this study does not depend solely on one to try to mitigate these issues.

Revolutionary Index Data Set

Data Sources and Justification

For the Revolutionary Index Data Set, the cases and factors examined will be limited, therefore there will be few metrics used. In order to calculate a revolutionary index score and compare the states that have documented cases of carrying out offensive cyber operations, the states used as cases in the data set are all of the states in the Council on Foreign Relations Cyber Operations Tracker. These nations have publicly documented cases of conducting offensive cyber operations, providing a baseline for who is capable of carrying out these kinds of attacks. All of the operations were attributed to these states, not necessarily concretely proven. The range of years examined for this study was also determined by the Cyber Operations Tracker, because it showed the first case of a state vs. state offensive cyber operations occurring in 2005, so that could be used as a reasonable baseline for when states became capable of carrying out these attacks.

This data set will be the one which examines the concept of revolutionary from the perspective that a *necessary* condition for offensive cyber operations to be considered revolutionary is that they should be used by weaker states to carry out attacks against stronger states. Since there are many factors that go into determining the strength of a state, and the main purpose of this study is not to determine state strength, this study utilized an already-established measure of state strength. The Correlates of War study has been carried out several times in several variations over the years, and the results have been widely respected for many years. This study will utilize the National Material Capabilities score that gives a Composite Index of National Capabilities (CINC) score that was completed in 2012. This score is determined utilizing six different variables: total population, urban population, iron and steel production, energy consumption, military personnel, and military expenditure.

The total number of operations for each year and the total number of targets per operation were also tracked for each state. These numbers are tracked in order to further examine trends.

Methodology

For each operation, the CINC score of the aggressor state is listed, as are the CINC scores for all of the target states of the operation. If the operation had more than one target state, the CINC scores of all of the targets were averaged into a single average CINC score for the targets. Then the CINC score of the aggressor was subtracted from the CINC score of the target(s) to determine the Revolutionary Index Score for that operation. If the Revolutionary Index Score is negative, then the aggressor was the stronger state, operating against a weaker state(s). If the Revolutionary Index Score is positive, then the aggressor state was the weaker state, operating against a stronger state(s). This Revolutionary Index Score is one metric that will be used to determine whether offensive cyber operations are revolutionary or not.

Another more general metric related to the Revolutionary Index Score is a more overarching perspective. It looks at all of the Revolutionary Index Scores for each state, and then averages them to get an average revolutionary index score for each state, which provides a more overarching view of the use of cyber operations by each state. This is a metric that will help measure the data on a state by state basis, as opposed to being broken down by individual operations for each state.

Revolutionary Capability Data Set

Data Sources and Justification

One of the difficulties with creating a Revolutionary Capabilities Data Set is determining whether or not states are capable of carrying out an offensive cyber operation, and the states that are capable would need to be included in the data set. There is no perfect threshold to determine this capability that is not actual observations of states carrying out the operations. The threshold that was established to decide whether states should be considered capable of carrying out a cyber operation was based on data found in the CIA World Factbook. If the listed military technology for the state was advanced enough to require sophisticated technological capabilities to operate and maintain it, then the state was included in the data set. The states that are listed as conducting offensive cyber operations in the Revolutionary Index Data Set, taken from the Council on Foreign Relations, are the states that are listed as conducting offensive cyber operations in this data set as well. Each data point represents a state, with the variables being measured by the most recent information for each state, and whether or not that state carried out an offensive cyber operation covered any operation it carried out through 2019. The list of states utilized in this study are listed in a table in the appendix.

The basic metric that is measured is for the main baseline of the study is whether or not the states carried out cyber operations. In order to put it in quantitative terms, the state is given a score of one if the state conducted an offensive cyber operation against another state. It is given a score of zero if it conducted no publicly documented offensive cyber operations. There is no acknowledgment of cyber operations conducted domestically in this data set because it is outside the scope of this study. This metric is the dependent variable.

There are four independent variables. The measure of level of democracy of each state comes from the Freedom House rating of the country from 2019. The state was given a score of two if Freedom House rated it completely free, a score of one if it was rated partly free, and a score of zero if it was rated not free. This will be used as a way to determine if there are any trends in level of democracy between the states that conduct cyber operations and those that do not.

A second independent variable is the GDP per capita of each state, to examine any correlations in economic factors that determined whether or not a state chooses to conduct an offensive cyber operation. The GDP per capita was measured in US dollars, and the data from 2019 was used. Measuring the GDP per capita is an imperfect measure of economic power because states with large populations might have low GDP per capitas but still have a large amount of economic revenue and power. Any measures of GDP and related economic measures have these imperfections, especially when attempting to compare states with vastly different economic situations. There may or may not be an economic point at which states choose to conduct these operations, but this will attempt to demonstrate whether or not there is.

The Composite Index of National Capabilities scores from 2012 explained in the Revolutionary Index Data Set section will be utilized in this data set as well. These CINC scores are used as a metric in this data set as an overall measure of state strength, to look for correlations in that area. The military power of states is difficult to measure, especially states that do not have extremely strong militaries and have similar strength to other states. This paper will utilize the measurement of the percentage of GDP per capita spent on the military in 2019 as a metric for measuring the strength of the military.

Methodology

This data set will be analyzed utilizing the statistical computer program R. The independent variables are listed above: GDP per capita (economic power), Freedom House score (level of democracy factors), CINC score (overarching state power), and percentage of GDP spent of the military (military power). The dependent variable is whether or not the state carried out an offensive cyber operation against another state. Since the dependent variable is measured in 0s and 1s as explained above, the data will be analyzed with a logit regression. First the variables will be vetted using the statistical program to ensure they can be used. If there are issues with the variables, they may still be able to be used because the spread of states is so large that there can be variation. Omitted variable bias is a possibility in this data set, but the main overarching subject areas have been covered. The field of study of offensive cyber operations is still forming and growing, so there is not an existing field of literature to determine the relevant variables. Therefore, this study attempts to cover an overarching view of all of the areas that could factor into the decision: economic power, military power, overall state power, and the level of democracy.

Once the variables are vetted and considered acceptable, the logit regression will be conducted. This regression will demonstrate which independent variables have the strongest relationship to the dependent variable. The independent variables will all be examined separately to determine if there is a relationship between them and the dependent variables. Then all of the relationships between the independent variables and the dependent variable will be compared against one another to determine which is the strongest and the best fit.

Hypotheses

There are many potential outcomes with the four different variables in this data set. The hypotheses of this paper are as follows:

H1: The higher the level of state power, the more likely that state is to carry out an offensive cyber operation.

H2: The higher the level of military power a state has, the more likely that state is to carry out an offensive cyber operation.

H3: The higher the level of economic power a state has, the more likely that state is to carry out an offensive cyber operation.

H4: The lower the level of democracy of a state, the more likely that state is to carry out an offensive cyber operation.

The opposite of this hypotheses may be true as well, but before carry out the statistical analysis, these are the hypotheses of this paper.

Chapter Four

Revolutionary Index Data Set Results

After the Revolutionary Index Data Set was created and the calculations were carried out, the data set was analyzed to determine the results. The main results are listed in the following table and will be analyzed and discussed immediately following the table. The more specific tables breaking down the scores and indexes for each state can be found in the appendix.

Revolutionary Index Overall Results	
State	**Average Revolutionary Index**
Australia	0.032781
Canada	0.030924
China	-0.145177
France	0.023427
India	-0.040029
Indonesia	-0.007149
Iran	0.050532
Israel	0.009568
Lebanon	0.044187
Netherlands	0.035942
New Zealand	0.039217
North Korea	0.045054
Pakistan	0.062580
Russia	0.006260
South Korea	0.053549
Spain	0.011283
Syria	0.134512
Taiwan	0.178149
United Arab Emirates	0.000951
United Kingdom	0.012904
United States	-0.10663
Vietnam	0.071101

In the final overall results of the data set, listed in the table above, there are twenty-two states. Out of those twenty-two states, four of them had negative average revolutionary indexes, while the other eighteen states had positive average revolutionary indexes. Therefore, four of the states on average were conducting offensive operations against states this study considers weaker than themselves, and the other eighteen on average conducted operations against states this study considers are stronger than themselves. This does not mean that every operation the state carried out was only against stronger states or weaker states, only that overall, they conducted more operations against states stronger than itself or were more significantly stronger than itself. However, these results are much more nuanced and require a closer examination. First, this section will walk through several example calculations for different states from the data set. Then, the next section will examine the overall trends more closely, in order to look through the nuances and attempt to determine what the data is truly showing. The chapter will then examine several case studies from the data set to support the overall trends. Finally, the chapter will conclude with a discussion of the results.

Example Calculations

The method for the revolutionary index calculations was explained in the previous chapter. This section will go through examples of these calculations step-by-step, demonstrating examples of individual revolutionary indexes and average revolutionary indexes.

The first example will be an offensive operation conducted by Canada in 2019. This operation was conducted against Russia, and targeted user accounts of Yandex, Russia`s search engine and email provider (Council on Foreign Relations, 2020). This was a one-to-one state operation, so it is a simple example. There was only one attack for Canada in 2019 (and overall in the data set), and its Correlates of War CINC score is 0.009155. Russia`s CINC score is 0.040079. To calculate the revolutionary index score, Canada`s CINC score was subtracted from Russia`s CINC score to demonstrate the difference in power between the states. In this case, the calculation was 0.040079 – 0.009155 = 0.030924. This demonstrates that Russia is stronger than Canada, with a difference in power of 0.030924. In this case, Canada was the weaker state conducting an offensive operation against the stronger state of Russia, demonstrated by the positive score.

China`s offensive cyber operation against India in 2013 provides an example of the calculation of a stronger nation attacking a weaker state. This offensive operation compromised the networks of India`s Defense Research and Development Organization for the purposes of espionage (Council on Foreign Relations, 2020). This was a one-on-one state operation as well, however China targeted many states in 2013. China`s CINC score is 0.218117. India`s CINC score is 0.080899. China`s score was subtracted from India`s score, with a calculation of 0.080899 – 0.218117 = -0.137218. This demonstrates that China is stronger than India, with a difference in power of 0.137218. The negative score indicates that China was the stronger state, conducting an offensive operation against the weaker state of India.

Many of the offensive operations conducted by various states targeted more than one target, up to at least twenty-one in some reported cases. An example of how a multi-target incident is a Russian threat actor, Red October, that carried out an offensive operation that targeted governments, diplomatic missions, academics, and energy and aerospace organizations around the world, and it affected fourteen target states. These states were Belgium, Armenia, Ukraine, Belarus, Kazakhstan, India, Iran, United States, Greece, Azerbaijan, Afghanistan, Turkmenistan, Vietnam, and Italy. Russia`s CINC score is 0.040079. To get a target CINC score, all of the CINC scores of the targets were averaged together with a calculation of (0.002928 + 0.000637 + 0.008231 + 0.001984 + 0.003103 + 0.080899 + 0.015763 + 0.139333 + 0.002971 + 0.001406 + 0.002734 + 0.015239 + 0.008844 + 0.012848) / 14 = 0.021209. Russia`s CINC score was subtracted from this average target score, with a resulting equation of 0.021209 – 0.040079 = -0.018870. This negative result demonstrates that Russia is stronger than its average target of that operation. It does not mean that Russia is stronger than each of the targets individually, simply stronger than the average target.

Revolutionary Index Overall Trends

The Revolutionary Index Data Set includes more states than are in the table at the beginning of the chapter, but not all of them had cases to include because they only carried out domestic offensive cyber operations, or they carried them out in 2020, which was outside the scope of this study. This study covered a fifteen-year period, from 2005 to 2019. A full list of the states included in the data set, including whether their revolutionary index scores were positive, negative, or if they do not have an index score is listed below:

State Summary Table			
State	**Score**	**State**	**Score**
Australia	*Positive*	North Korea	*Positive*
Canada	*Positive*	Pakistan	*Positive*
China	*Negative*	Palestine	*N/A*
Egypt	*N/A*	Panama	*N/A*
Ethiopia	*N/A*	Russia	*Positive*
France	*Positive*	Saudi Arabia	*N/A*
Hong Kong	*N/A*	South Korea	*Positive*
India	*Negative*	Spain	*Positive*
Indonesia	*Negative*	Syria	*Positive*
Iran	*Positive*	Taiwan	*Positive*
Israel	*Positive*	Turkey	*N/A*
Kazakhstan	*N/A*	Uganda	*N/A*
Lebanon	*Positive*	United Arab Emirates	*Positive*
Mexico	*N/A*	United Kingdom	*Positive*
Morocco	*N/A*	United States	*Negative*
Netherlands	*Positive*	Uzbekistan	*N/A*
New Zealand	*Positive*	Vietnam	*Positive*

To summarize, out of the thirty-four states on the list in the data set, four of the states had negative revolutionary indexes, eighteen had positive revolutionary indexes, and twelve do not have revolutionary indexes due to the lack of qualifying incidents.

There were three hundred operations recorded in the data set. When looking at the breakdown of the individual incidents, 67.6% of the offensive operations had negative revolutionary indexes, demonstrating that in 67.6% of the incidents in the data set, a stronger state conducted an operation against a weaker state. The other 32.3% of operations were conducted by a weaker state against a stronger state, therefore had a positive revolutionary index score.

Of the eighteen states with positive revolutionary indexes, ten of the states were only reported to have carried out one offensive operation (though not necessarily only one target state) over the fifteen-year period. Fifteen of the eighteen states conducted seven or less offensive operations. Of the three out of eighteen states that carried out more than seven offensive operations, their numbers of offensive operations were significantly higher at twenty-seven, thirty-six, and seventy-five, belonging to North Korea, Iran, and Russia respectively.

There were four states with negative revolutionary index scores, with a wide range of number of operations carried out by each state, which range from one offensive operation to one hundred eighteen operations. India and Indonesia each only carried out one offensive operation (though not necessarily one target state), while the United States carried out thirteen operations, and China carried out significantly more, at one hundred eighteen operations. The high number of offensive operations carried out by China skews the data set, but also demonstrates the conclusions of the data set, which will be discussed in the next section.

There was also a wide variety of the number of targets of each operation. For the three hundred offensive operations, there were eight hundred forty-two targets. This comes out to an average of 2.8 targets per operation. Many operations only targeted one state, however many also targeted more than one target state. The highest number of targets recorded in one operation was twenty-one targets.

Revolutionary Index Case Studies

There were three hundred offensive operations carried out by twenty-two states. This section will discuss some of the operations carried out, including some operations that were carried out by multiple states against one target state. These operations are listed and counted separately in the data set to account for the different states that carried them out, however they are the same operation and could be useful to discuss together. Each of the examples will help demonstrate how the revolutionary index scores for that incident contributed to the state`s average revolutionary index score.

In 2019 several states together conducted an offensive operation against Russia`s search engine and email provider, Yandex. This operation was suspected to have been in order to compromise and gain access to user accounts (Council on Foreign Relations, 2020). These states included Australia, Canada, New Zealand, the United Kingdom, and the United States. This operation was the only operation that several of the states were reported to have carried out, including Australia, Canada, and New Zealand. Due to Russia`s CINC score of 0.040079, this caused a result of a positive revolutionary score for Australia, Canada, New Zealand, and the United Kingdom due to their CINC scores of 0.007298, 0.009155, 0.000862, and 0.015277, respectively. Only the United States had a negative revolutionary index score for this operation due to its CINC score of 0.139333.

China was the most prolific user of offensive cyber operations in the data set, as well as the state with the highest CINC score. Therefore, any operation it carried out resulted in a negative revolutionary index score, leading to the assumption that any operation it carried out was against a (at least relatively) weaker state, including the United States. An example of this is demonstrated by the compromise of the United States government`s Office of Personnel Management in 2015. As a result of this operation, China had access to the records and personal information of millions of United States government employees (Council on Foreign Relations, 2020). When China`s

CINC score of 0.218117 is subtracted from the United States` score of 0.139333, the result is a negative revolutionary index score of -0.078784. The United States is the state with the closest CINC score to China, so this is the lowest difference in power between China and another state and demonstrates the trend in how China`s offensive operations will be scored and recorded.

France was only reported as carrying out one offensive operation, which was an overarching operation carried out by its government against a wide range of target states and industries. Its state targets included Syria, the Netherlands, the United States, Russia, Spain, Iran, China, Germany, Algeria, Norway, Malaysia, Turkey, the United Kingdom, and Greece. The industries targeted by the operation included governments, private industries, media organizations, military organizations, and humanitarian organizations (Council on Foreign Relations, 2020). France has a CINC score of 0.014207, and the average of its target states` CINC scores was 0.037634, giving the operation a positive revolutionary index score of 0.023427. Although many of the target states were weaker than France, due to the much larger CINC scores of mainly the United States and China, the overall target CINC score came out to be higher than France`s, giving a positive revolutionary index score.

India and Indonesia are the only two other states besides China and the United States that have calculated negative revolutionary index scores. India is recorded as having carried out one offensive cyber operation, against four states: the United States, Pakistan, Bangladesh, and Sri Lanka. Although the United States is notably stronger than India, the large difference in power between India and the other three states is large enough that it resulted in an overall negative revolutionary index score. Pakistan, Bangladesh, and Sri Lanka have CINC scores of 0.014554, 0.007469, and 0.002123, much lower than India`s CINC score of 0.080899. This gave India an overall negative revolutionary index, demonstrating that India conducted offensive operations against weaker states more frequently than against stronger states. Indonesia only has one recorded offensive operation, which was conducted against Australia. With Australia`s CINC score of 0.007298 and Indonesia`s CINC score of 0.014447, it gives Indonesia a negative revolutionary index score. While this one operation may not be significant, the fact that the one operation was against a weaker state is significant, because it shows the priorities for Indonesia. Its place as one of the four states with negative revolutionary indexes is not insignificant.

Iran, North Korea, and Russia are the three states with positive revolutionary indexes and high frequencies of operations. They all conducted operations against a wide range of target states, and conducted both one-on-one operations, and operations against many states, including both weaker and stronger states. The main target that helped cause these states to have overall positive revolutionary index scores was that they each conducted many operations against the United States, a state with a much higher CINC score.

Israel has an overall average positive revolutionary index score, indicating that it primarily conducts offensive operations against states stronger than itself. For example, its operation against Iran in 2015 to gain information regarding the Iranian nuclear deal discussions showed its use of offensive cyber operations against a stronger state. Israel has a CINC score of 0.004250, while Iran has a CINC score of 0.015763, resulting in a positive revolutionary index score.

There are other states in the data set, however they fit within the patterns described above, and do not require specific explanations. These examples have demonstrated how the scores and strength determinations are made, and the next section will discuss these scores and their meanings.

Discussion of Revolutionary Index Data Set Results

The results of the revolutionary index data set provide some trends, but overall leads to more questions than answers. Despite this, it gives the study of offensive cyber operations a starting point, and there are some conclusions that can be drawn from it. The lack of publicly available information on offensive cyber operations will always cause large gaps in the understanding of the subject. However, even if all of the information was publicly available and there was a clear picture of the incidents occurring, there still might not be a clear trend or predictable behavior. This paper aims to at least create a starting point for understanding how offensive cyber operations have been used by states, and how and by whom they will be used in the future.

As seen in the tables above, there are four states with negative revolutionary index scores, and eighteen with positive revolutionary index scores. The four states with negative revolutionary index scores are China, India, Indonesia, and the United States. The eighteen states with positive revolutionary scores are Australia, Canada, France, Iran, Israel, Lebanon, the Netherlands, New Zealand, North Korea, Pakistan, Russia, South Korea, Spain, Syria, Taiwan, United Arab Emirates, United Kingdom, and Vietnam. As previously discussed, even though there are a much greater number of states that carried out operations against states stronger than themselves, simply looking at that statistic is misleading.

Out of the eighteen states with positive revolutionary indexes, only eight carried out more than one offensive cyber operation over the fifteen-year period (though not necessarily only one target state), and only three carried out more than seven offensive cyber operations. North Korea conducted at least twenty-seven offensive cyber operations, Iran carried out at least thirty-six, and Russia carried out at least seventy-five. There are many potential reasons for the wide range of operations carried out by each state, and some will be discussed when examining the second data set in the next chapter.

States With Positive Revolutionary Index Scores

The following subsections will discuss states that on average had positive revolutionary index scores and examine possible trends. These states on average conducted offensive operations against states considered stronger than them by the data set, through the use of Correlates of War CINC scores. Since Iran, North Korea, and Russia carried out the largest number of offensive cyber operations of those with positive revolutionary index scores by far, they will each be examined individually. Then the remaining states will be examined as groups, first the states that carried out more than one offensive cyber operation, and then those that only carried out one recorded offensive cyber operation.

North Korea

Out of the three positive score states with higher numbers of offensive operations, North Korea had the lowest number at twenty-seven recorded incidents. North Korea`s complete technological capabilities are unclear, but it is clearly capable of carrying out offensive cyber operations and has been since at least 2009. It has carried out a wide range of operations against a wide range of targets. There are several possible reasons for North Korea`s reliance on offensive cyber operations, and the choice of targets for these operations.

North Korea will always be an outlier and difficult to categorize due to the secrecy of the regime and its priorities. Though it is an economically poor state, North Korea focuses its resources on its military, including its offensive cyber capabilities. It conducts these offensive cyber operations in a variety of ways, including financial theft, espionage, denial of service, and doxing. These operations are conducted against a wide range of target states, ranging from economically and militarily weak states to major world powers.

Over the past several years, North Korea has utilized hacking groups managed by its intelligence services to rob banks around the world. They utilize these techniques for financial gain, which could be part of their strategy to get around financial sanctions imposed on them from states around the world, including the United States. The groups have targeted financial institutions in a wide variety of states, from economically poor nations with poor security for their financial institutions to rich states with robust cybersecurity systems for their financial institutions. North Korea targets the financial institutions of any state where it can find the opportunity and foresees significant financial gain. Cyber tactics allow North Korea to carry out these operations more easily, and they likely would not be able to carry out these operations without the cyber realm. Otherwise, it would be much more logistically difficult to target physical institutions all around the world.

In 2014, North Korea carried out a doxing operation against Sony Pictures in the United States, in response to their film *The Interview*, about two reporters attempting to assassinate Kim Jong-Un (Sethi, 2020, 160-182). This was a political statement, and an aggressive action that North Korea was able to get away with due to its nature. The release of the film was greatly subdued, and though it was still released, North Korea was effectively able to censor the release of a movie in a democratic country. There were few, if any, consequences to this operation for North Korea. This was a demonstration of North Korean power against a stronger state (the United States) that resulted in a positive revolutionary index score.

Many of North Korea`s offensive cyber operations have been carried out against the United States, which helped ensure that it ended with a positive revolutionary index score since the difference in power and CINC score is so great. This demonstrates how cyber methods enabled a weaker state that aspires to be powerful to carry out operations against a major world power with few consequences. North Korea has used denial of service and doxing operations to get its political message across, as well as espionage in order to gain access to the information of private industries and government entities in the United States. While the United States has been the main major power target of North Korea`s cyber operations, China and Russia have been targeted several times as well. The United States is likely targeted much more frequently because it is much more of an adversary of North Korea. These operations allow it to carry out offensive action against any major powers; however, the gains these operations give North Korea are small. North Korea has never attempted (at least not based on publicly available information) to initiate or carry out anything resembling cyber war. This indicates that cyber operations might be useful offensively, but they have not completely changed the face of warfare.

Although North Korea`s cyber operations have targeted a wide range of states, most of the operations targeted the United States, South Korea, and other regional rivals in Asia. Its consistent targeting of South Korea also helped lead to its average positive revolutionary index score, since North Korea has a CINC score of 0.013260, and South Korea has a CINC score of 0.023212. Targeting South Korea and other regional rivals in Asia helps support the idea of cyber capabilities being a regional tool that can help states gain power over other peer competitors that are geographically close. North Korea cannot physically attack South Korea, and likely has some difficulty crossing the border to commit espionage physically. Therefore, cyber operations are likely a useful tool to conduct offensive operations against a neighboring rival and gain useful information to use against them.

North Korea is a nuclear power with several missile options, with strong intentions to develop more. This capability makes them a threat to stronger states; however, they likely only have a small number of nuclear-capable missiles with usable ranges. North Korea likely not only utilizes offensive cyber operations for financial gain and espionage, but also to force major world powers to see them as a threat, a force to be taken seriously. Though their cyber operations have caused some financial and data losses, these operations have been more of a “nuisance” than causing true damage. Cyber operations have allowed North Korea to “poke” major powers and remind them of North Korea`s power aspirations without forcing the stronger states to respond or conduct operations in response. Due to the lack of true, lasting damage caused by these cyber operations, and the lack of evidence that North Korea could carry out extremely sophisticated, disabling operations on a target state-wide or even government-wide, there has been no indication that North Korea`s cyber capabilities could carry out an equalizing operation against a stronger state.

Though North Korea has carried out offensive cyber operations against the United States, they were either for the purposes of espionage or to send a political message, which generally resulted in more of a nuisance than destruction. This does not speak to cyber tactics being a revolutionary tool of warfare, because it has not given it relatively equal standing to a major power such as the United States, Russia, or China. Cyber capabilities might progress further to make this true, but they are not to that point yet.

Iran

Iran has been conducting offensive cyber operations since at least 2010, against a wide variety of target states around the world. Out of the three states with positive revolutionary index scores and high numbers of operations, Iran conducted the second most offensive cyber operations at thirty-six. There are many potential reasons for this trend, and the motivations are likely similar to those of North Korea. As more of a medium power in the world, Iran does not have the physical capabilities to target major world powers conventionally. It also has many regional rivals, which they likely could not attack conventionally without sparking a larger conflict.

While Iran might not be a major power in the world, it is a relatively major power in the Middle East, with many rival states in the region. One rival state that Iran has targeted with its offensive cyber operations is Bahrain. Bahrain was included in several of Iran`s operations that targeted many states at once, as well as targeted Bahrain directly in deliberate efforts against the state. In 2019, threat actors attributed to Iran targeted Bahrain`s National Security Agency, Ministry of Interior, and the office of the first deputy prime minister (Council on Foreign Relations, 2020). In 2020, an Iranian state-backed group installed malware on the network of Bahrain`s national oil producer (Council on Foreign Relations, 2020). Although the 2020 operation is not included in the data set, it is worth noting since it demonstrates a pattern. While these operations were detected, it is unclear how much information Iran gained as a result. Iran has used offensive cyber operations to gain advantages over regional rivals, including both weaker rivals and stronger rivals.

Another frequent target of Iran`s cyber operations is Saudi Arabia, a major regional rival. Saudi Arabia is considered stronger than Iran, and Iran has utilized cyber operations to carry out offensive operations without prompting a conventional response from Saudi Arabia. Iran has carried out many cyber operations against Saudi Arabia since 2010, and one of the most notable was in 2012, when threat actors attributed to Iran wiped data from approximately 35,000 computers belonging to the Saudi state-owned oil company Aramco, one of the world`s largest oil companies (Council on Foreign Relations, 2020). This was a clearly offensive operation that destroyed data, which would have likely prompted a military response if the computers had been physically destroyed, but since there had been no physical intrusions, Saudi Arabia`s response appeared to only be denouncement. Cyber operations have allowed Iran to conduct operations against Saudi Arabia, a major regional rival, that have been damaging, as well as espionage, with few public consequences, though this does not mean there were no consequences over all.

There have been a number of cases of Iran conducting offensive cyber operations against multiple states at a time, and in many cases, against groups of states in the Middle East. These cyber operations can be seen as aiding Iran`s place in the Middle East as a powerful actor, one that must be considered when acting in the region. It could help keep Iran in front of those states in the region that have not yet developed cyber capabilities. It could also help Iran compete with regional rivals that are more at the peer level, such as Saudi Arabia and Israel. These cyber operations have allowed Iran to conduct offensive operations to attempt to increase its power without firing a shot, and without prompting a response from the other states.

Although Iran has been working on developing nuclear capabilities for many years now, it has not been successful, so it does not have nuclear capabilities to rely on to be taken seriously by the major world powers as North Korea does. While Iran is working to develop nuclear capabilities and improve its conventional capabilities, its cyber capabilities are likely helping its position against the major powers, but these capabilities are not equalizing. Iran has not conducted any offensive cyber operations that would qualify as cyber war, and no truly disabling operations against major powers. They operations have also been conducted without consequences. It has conducted cyber espionage against major powers that might have yielded useful information; however, none of the cyber operations were truly destructive against a major power such as the United States, China, or Russia.

Iran`s use of offensive cyber operations against major powers could lead to the assertion that these are revolutionary tools of warfare. These operations do demonstrate the standing and abilities that they can give a medium-sized power. However, to date they have not proven to be an equalizing factor. Iran`s station in the world power order has not risen past a medium power, and they have not carried out any true, destructive cyber attacks against a major power. Cyber tactics have allowed Iran to carry out espionage more deeply than it might have otherwise, but these operations indicate that cyber tactics are simply a new way to carry out espionage.

Russia

Russia was once one of the two great powers in the world, in constant competition with the United States throughout the Cold War for power. Out of all of the states with average positive revolutionary index scores, Russia had the highest number of offensive cyber operations, at seventy-five. Russia has the highest CINC score out of all of the states with positive revolutionary index scores, so it is unsurprising that it was the most aggressive. It carried out operations against a wide range of states, and many of its offensive cyber operations were carried out against the United States, which solidified its positive revolutionary index score since the United States has a higher CINC score than Russia. However, Russia also carried out destructive operations against weaker states, such as Estonia and Georgia.

As discussed in the introduction, in 2007 actors attributed to Russia carried out a distributed-denial-of-service operation against Estonia. This operation lasted for days, disrupting access to Estonian services from both private and public entities, including government services. These denial-of-service attacks are estimated to have had an economic impact of twenty-seven to forty million US dollars (Haataja, 2017, pp. 160-161). This was not a physically destructive operation, but it was very disruptive and had a great economic impact. Though Russia on average conducted operations with positive revolutionary index scores, this operation resulted in a negative revolutionary index score because Russia is much stronger than Estonia. This is significant because although Russia generally targets stronger states with its offensive cyber operations, one of its most damaging operations was against a much weaker state.

Another example of a Russian offensive operation against a weaker state was one of the first examples of offensive cyber operations potentially being used to coincide with offensive operations in a conventional war. In 2008, Russia invaded Georgia, but not before conducting denial-of-service attacks that disabled Georgian websites and put out pro-Russian propaganda before the invasion (Council on Foreign Relations, 2020). Though these operations were conducted, they likely did not have a large impact on the outcome of the war itself. This is a significant example because it demonstrated that cyber operations could be used together with conventional tactics in a wartime situation, but they were still not truly utilized or fully integrated. This could have been considered cyber warfare in some respects, but the publicly known damage was so superficial and relatively insignificant that it does not meet that threshold, though the operations do qualify as cyber attacks. Another reason for its significance is that this is another of Russia`s most significant operations, but it was once again carried out against a significantly weaker state. This also supports the idea that the most damaging non-espionage operations are generally carried out against weaker states.

In contrast to significant operations against weaker states, Russia has also carried out a number of operations against stronger states, predominantly the United States. These operations have been carried out against a wide range of entities in the United States, private sector, universities, public sector, the government, and the military.

Several of these operations were carried out against the Democratic National Committee, directly against the committee and against the Democratic National Convention. Most operations conducted by Russia against the United States are for the purposes of espionage, and these operations are the reason that Russia ended up with a positive revolutionary index score.

Though the operations by Russia against the United States could lead to the assumption that offensive cyber operations are a revolutionary tool, this needs to be examined more closely. The operations against Estonia and Georgia demonstrate that at the very least there is potential for disruptive use of cyber tactics in warfare, possibly even destructive uses for cyber tactics in warfare. However, these tactics have only been partially utilized, and only against weaker states. When conducting operations against stronger states or other major powers, cyber operations seem to merely be used as another tool of espionage. While this could potentially be seen as a revolution in tools of espionage, this indicates that it might not be a revolutionary tool of warfare itself at this point.

Despite the fact that Russia`s cases of offensive cyber operations might not meet the qualifications to be considered a revolutionary tool of warfare, these operations have allowed Russia to continue to assert its status as a threat and a major power in the world. Cyber operations are more difficult to concretely prove attribution, and Russia has been able to use this aspect to conduct operations while claiming innocence and prevent retaliation. Russia has nuclear weapons that could be considered a threat to almost any nation worldwide; however, it is unlikely that these weapons will be used in conflicts due to their major escalatory effect. Russia`s ability to carry out cyber operations allows it to be a clear and present threat to major powers and other states around the world.

Overall Trends of Positive Scores With High Numbers of Offensive Cyber Operations

The three states with the highest numbers of offensive cyber operations were all within the top seven CINC scores of the eighteen positive score states. Russia had the highest CINC score, Iran had the third highest, and North Korea had the seventh highest. These states were already relatively "strong" states and had some sort of standing and military power. Russia and Iran clearly fit this model; however North Korea is somewhat an outlier.

North Korea is economically weak, and its only military standing essentially comes from its nuclear weapons capabilities. Iran lacks nuclear capabilities; however, its conventional military capabilities and its progression towards nuclear capabilities give it military standing. Russia`s status as a major world power is clear, though it is not the world power that it was thirty to forty years ago. Cyber capabilities might help these states keep their current status, or remain a threat to stronger world powers, but it has not given these states an equalizing power.

All three of these states have heavily used cyber operations for the purposes of espionage. This leads to the idea that cyber tactics might be a revolution in espionage tactics, even if they have not yet crossed the threshold to be considered revolutionary tools of warfare. They have allowed states to conduct espionage against states and gain information from them without stepping foot in the country in many cases. This requires less resources from the states, and potentially less consequences if they are caught, because the attribution problem allows for deniability.

North Korea and Iran focused many of the offensive cyber efforts against regional rivals, both stronger and weaker than themselves. Offensive cyber operations could allow states to maintain their regional superiority, or at least preserve their sovereignty against potential regional threats. It could also potentially allow states to try to undermine their rivals without their knowledge. Russia targeted some states in Europe and along its borders as well. With the exception of the consistent targeting of the United States by these three states, they mostly focused on regional threats, which could take away from the potential truly revolutionary capabilities of cyber operations.

The consistent targeting of the United States could be seen as evidence that offensive cyber operations are revolutionary tactics, but not necessarily revolutionary tools of warfare. Cyber operations have allowed weaker states to target the United States, which is a shift from before cyber operations, when states had to carry out physical damage or infiltrate a state in order to target that state. Cyber tactics have allowed states from around the world to target the United States without setting foot in the country. However, these tactics still have not truly undermined the power of the United States or caused a shift in power, nor have they been used as an actual form of warfare against the United States. Cyber operations may be used as a major tool of warfare in the future, or they may become advanced enough to control the infrastructure and systems of a state, but they are not to that point yet, therefore they should not yet be considered a revolution in military affairs.

States With More Than One Offensive Cyber Operation

There are five states in the data set with a positive revolutionary index score on average that have carried out more than one offensive cyber operation, but less than ten offensive cyber operations: Israel, Pakistan, the United Arab Emirates, the United Kingdom, and Vietnam. Though they carried out few operations, on average these states carried out operations against stronger states.

Most of Israel`s offensive cyber operations were conducted against regional rivals. The most frequent target of Israel`s offensive operations was Iran, a state with a stronger CINC score than Israel. Both Israel and Iran are middle powers, though at differing levels. These operations have allowed Israel to challenge Iran`s power in the region, and several of these operations have targeted Iran`s nuclear program. Israel`s operations support the idea that offensive cyber operations are useful against regional targets, as well as states at a similar power level. Israel`s participation in the Stuxnet operation against Iran (which will be discussed in more detail in the United States section) could be considered revolutionary, but it was carried out with a state stronger than Iran, so that could take away some of the revolutionary factor. If Israel is able to use these operations to gain power going forward, then that could help indicate that the tactics are revolutionary.

The main target of Pakistan`s offensive cyber operations have been regional actors, especially India. India has a much higher CINC score than Pakistan, so this difference was a major factor in Pakistan`s revolutionary index score. Pakistan and India have been significant rivals for a long period of time, and cyber operations are another way that they can target one another. Cyber operations could be seen as a revolutionary tool of warfare in this conflict because they can inflict damage against one another without firing a shot, which could take the conflict to a new arena. This helps emphasize the regional conflict potential of offensive cyber operations, and the India/Pakistan conflict will likely be an interesting area to watch going forward to see how and if it incorporates cyber operations.

The United Arab Emirates has exclusively conducted offensive cyber operations against regional rivals: Qatar, Turkey, and Yemen. Though the United Arab Emirates is rated as stronger than Qatar and Yemen, the power and score differential between the United Arab Emirates and Turkey is enough to sway its average revolutionary index score in the positive direction. The variation in conducting operations against both stronger and weaker states, but all of the targets are regional rivals is significant and demonstrates the purpose for which cyber operations are currently used by that state. This use of cyber operations is not changing the balance of power in the region, leading to the conclusion that the example of the United Arab Emirates does not support the idea that cyber operations cause a revolution in military affairs.

The United Kingdom carried out two offensive cyber operations. One was against a wide range of state targets, and the other only targeted Russia. Russia is considered stronger than the United Kingdom, which helped solidify the United Kingdom`s positive revolutionary index score. Russia being one of the main focuses of the United Kingdom`s cyber operations is significant because the United Kingdom seems to focus its efforts (though a small number of operations) against a major power that is considered stronger than itself. The United Kingdom itself is a relatively major power in the world, so it supports the idea that states that already have power utilize cyber operations to compete with other states with power. These cyber operations have allowed the United Kingdom to conduct espionage against Russia but have not given the United Kingdom an equal power to Russia. This leads to the conclusion that the cases of the United Kingdom do not support the assertion that offensive cyber operations are revolutionary tools of warfare.

Vietnam targeted a variety of states with its offensive cyber operations, but mainly regional rival states as well. This supports the idea that to date, cyber operations have mostly been utilized in regional rivalries. These conflicts could prove that cyber operations are revolutionary in the future if cyber operations change the balance of power in those conflicts, however, this has not happened to date.

States With Only One Offensive Cyber Operation

There are ten states in the data set with a positive revolutionary index score on average that have carried out only one offensive cyber operation (though not necessarily one target of the operation): Australia, Canada, France, Lebanon, the Netherlands, New Zealand, South Korea, Spain, Syria, and Taiwan. These states only carried out one offensive cyber operation each, though not necessarily against one target state. If there was only one target of the operation, then that one target was stronger than the aggressor state. If there was more than one target state of the operation, then the average of all of the CINC scores of the targets resulted in an average score stronger than the score of the aggressor state.

Australia, Canada, the Netherlands, and New Zealand all only targeted Russia with their one offensive cyber operation, though they were not all part of the same operation. The Netherlands conducted its own operation against Russia, while Australia, Canada, and New Zealand (the United Kingdom also took part in this operation) conducted a joint operation against Russia. This is significant that the only offensive cyber operation that these states carried out was against a stronger state, a major world power. These states would likely be considered middle powers, not weak, but by no means strong. Cyber operations have allowed these states that already have some level of power to conduct operations against a major power but have not changed the balance of power.

France and Spain both carried out an operation against a wide range of targets of varying levels of power, and both ended up with the average CINC score of the states of that list being higher than their own. Neither of these cases help either support or disprove that cyber operations are revolutionary tools, because the wide range of strengths of the target states seems to be random, there is not a pattern. This could be a sign that these tactics are not revolutionary because there is not a clear pattern of weaker states conducting operations against stronger states, but the lack of a pattern in this case does not count as evidence for or against the argument.

Lebanon carried out a single operation that targeted the United States, France, Germany, and Canada, all more powerful than itself. This operation was for the purposes of espionage, indicating that although it was conducted against significantly stronger states, its purpose was not revolutionary. This instance of an offensive cyber operation was purely a new way to conduct espionage, it was meant to be covert, and it did not help Lebanon gain any more power.

South Korea`s one offensive cyber operation supports the idea that these tactics are most useful against regional state rivals. The operation was conducted against China, North Korea, Russia, Japan, and Taiwan. All of these states are geographically close to South Korea, and all of them, except potentially Japan, are significant rivals of South Korea. The purpose of the operation was espionage, indicating that there was no expected power shift from the operation. Cyber tactics have likely allowed South Korea to conduct more espionage on those other states than it might have been able to otherwise, but this does not mean that it is revolutionary because it does not change the distribution of power in the region.

Both Syria and Taiwan only carried out one offensive cyber operation each, and each of these operations targeted a major power. Syria`s was an espionage operation against the United States, while Taiwan conducted a denial-of-service operation against China. Syria`s espionage operation reinforces the idea that although weak states may consider targeting strong states, if they do carry it out it will be for espionage to gain information, not to take advantage and change the balance of power. Although Taiwan conducted a truly offensive cyber operation against China that could qualify as revolutionary, it occurred in 2007 and Taiwan has not carried out another offensive operation since then. If cyber operations were truly revolutionary, these operations would have continued and likely become more aggressive over time.

If these offensive cyber operations caused a shift in the balance of power, then these tactics might qualify as revolutionary. However, none of the cyber operations described in this section show evidence that the balance of power shifted as a result of these operations. Another sign that these tactics are revolutionary would be if they were used by these states more frequently as time progressed. The length of the list of states that carried out less than ten cyber operations throughout the fifteen-year period itself indicates that they are not being utilized as frequently as they should be if the tactic was truly revolutionary. The consistent use of these operations for the purposes of espionage indicates that they are still being used for non-cyber attack/cyber warfare purposes.

States With Negative Revolutionary Index Scores

There were four states with negative revolutionary index scores, with a wide range of number of operations carried out by each state, which range from one offensive operation to one hundred eighteen operations. India and Indonesia each only carried out one offensive operation (though not necessarily one target state), while the United States carried out thirteen operations, and China carried out significantly more, at one hundred eighteen operations. The high number of offensive operations carried out by China skews the data set, but also demonstrates the conclusions of the data set, which will be discussed going forward.

India

India only conducted one offensive cyber operation against several targets, mainly regional rival actors. India is one of the strongest actors in the region and its CINC score reflects that, so it was stronger than most of the targets of its operations. One of the targets of its operation was Pakistan, its biggest rival, who is rated as weaker than India. Cyber operations have allowed India to act against Pakistan, who they likely could not act against conventionally without a strong, serious response. The purpose of the cyber operation was espionage, but that could have helped India gain an advantage over Pakistan. However, if cyber operations were truly revolutionary, there would have been more than one instance of India using these operations against Pakistan to gain an advantage. It is highly likely that they have used these operations against Pakistan on other occasions, but they have not been publicly recorded if they have happened, so it is not able to be used as evidence for this paper. As stated earlier when discussing Pakistan, this rivalry/conflict between India and Pakistan will be a good power struggle case to watch moving forward for the potential for the use of offensive cyber operations in warfare, or in lieu of warfare, in the future.

Indonesia

Indonesia conducted one recorded offensive cyber operation against one state over the fifteen-year period examined. It conducted this offensive operation against Australia, a state with a weaker/lower CINC score than Indonesia, giving Indonesia an overall negative revolutionary index score. The purpose of this operation was espionage, indicating that even though the operation was carried out against a weaker state it was still for the purpose of espionage. This example does not support that these operations are revolutionary, because there was only one operation carried out by Indonesia, and it did not affect its power difference with Australia.

United States

The United States only carried out thirteen recorded offensive cyber operations over the fifteen-year period. Most of these operations were carried out against weaker states, because the only state with a higher CINC score than the United States is China. The United States is only publicly listed as carrying out one cyber operation against China, so that was the only incident with a positive revolutionary score, all other operations ended with a negative revolutionary score, giving the United States an overall negative revolutionary index score. Out of the thirteen offensive cyber operations, less than half of the overall operations were for the purposes of espionage. The espionage operations were conducted against a large number of states at once. Most of the operations were truly offensive, using tactics such as data destruction, sabotage, and denial-of-service.

One of the most notorious and successful examples of an offensive cyber operation carried out by the United States was Stuxnet. This operation used cyber means to conduct sabotage against the Iranian nuclear program. The Stuxnet "worm" was found in computer systems all over the world but was designed to only target a specific industrial controller designed to run a series of nuclear centrifuges manufactured by the company Siemens. These devices were utilized by Iran in their nuclear program that the United States wanted to prevent. The "worm" caused the centrifuges to make tiny adjustments to the pressure inside the centrifuges and caused the speed of the centrifuges to speed up and slow down, breaking or exploding the centrifuges and causing damage to the overall machine (Singer and Friedman, 116-117).

Stuxnet was one of the first, if not the first, examples of a successful offensive cyber operation that caused physical damage and went largely undetected for a long period of time. The Stuxnet operation could be seen as more effective than a physical attack could have been, because it took longer to discover and fix, potentially setting back the program for a longer period of time than if the United States had physically attacked the Iranian nuclear facilities when the operation first began. It also allowed the United States to deny the operation for a long period of time and made it more difficult for Iran to retaliate. If the United States had physically attacked the Iranian nuclear facilities, Iran could have responded aggressively with a physical attack of their own or could have had the international community admonish the United States more thoroughly. Since this type of operation was so new, the international community had a difficult time responding, and Iran could merely denounce the operation, they did not (at least publicly) carry out any operations in retaliation.

The United States carried out two very public denial-of-service operations against adversary states: an operation against North Korea in 2017, and a 2018 operation against a Russian troll farm that was reported in 2019. The United States publicly announced that they were conducting denial-of-service operations against North Korea`s General Reconnaissance Bureau, a branch of their intelligence services. In 2018, United States Cyber Command (CYBERCOM) began a denial-of-service operation against Russian troll farms known for using disinformation tactics. The operation against Russia was technically in retaliation for offensive cyber disinformation operations conducted by Russia, so it could potentially be seen as cyber retaliation for a cyber operation. Both the operation against North Korea and the operation against Russia were public offensive operations carried out by one state against another, that did not cause a physical response and neither state appeared to respond.

The United States demonstrates several different aspects to consider about offensive cyber operations. The ways in which the United States has utilized offensive cyber operations could be considered revolutionary because they have conducted truly offensive operations, some of which have caused physical damage, against other states. The Stuxnet operation was a prime example of how a cyber operation could cause physical damage, and since this operation occurred back in 2010, it could be assumed that in the ten years since this point, there could be cyber tactics even more advanced and better at causing physical damage.

The public denial-of-service operations against North Korea and Russia carried out by the United States demonstrates how states can utilize cyber operations without fear of another state responding. They also allow the United States to compromise infrastructure and systems within the sovereign borders of the target state(s). This could be seen as a violation of sovereignty of the target state, which could prompt a response. However, as seen throughout the examples throughout the data set, there is typically not a response stronger than denouncement, and regularly no response at all.

Despite all of the potentially revolutionary offensive cyber operations the United States has carried out, it could be argued that because these operations were carried out by the United States, a major power, this supports the argument that cyber operations are not revolutionary. If the technology was truly revolutionary, this type of operation would be used by a wide variety of states, especially states weaker than major powers. The United States has used cyber technology to assert power over aspiring middle powers that want to become major powers, and against lower powers as well. This supports that cyber operations are simply another tool used by the strong powers to keep the weaker powers in their current position, or at least to prevent them from becoming major powers. These instances give evidence both for and against the revolutionary potential of offensive cyber operations; however, since "revolutionary" in the sense of this paper is dependent on which states actually use cyber operations and how they change the existing status quo or balance of power, the evidence that the truly offensive types of cyber operations that could be considered cyber attacks are more frequently carried out by states that are already major powers.

China

As the state with the highest CINC score, every offensive cyber operations that China carried out was against a state considered weaker than themselves, giving all of their operations a negative revolutionary index score. China carried out several different types of cyber operations, but most of the operations it carried out were categorized as espionage operations. Many of its operations were carried out against the United States as well. Both the fact that many of China`s operations were likely for the purposes of espionage and that many of the operations were carried out against the United States are significant, but first there will be an examination of several different examples of Chinese state-sponsored offensive cyber operations.

China was able to successfully target and penetrate the Office of Personnel Management of the United States government. The operation was discovered in 2015, but it is unknown or not public knowledge how long China had been in the system and what information they had gained access to, but it is known that they gained access to the security clearance information of tens of thousands of United States government employees. The security clearance information in the system contained potentially damaging personal information that the Chinese government could use to its advantage. The ambiguity of what information China was able to gain access to, exploit, and save increases the damage of the operation because what China is planning to do or could do with the information is unclear (Schmidt, 2015). This is an example of China conducting espionage against a fellow great power, indicating that offensive cyber operations might not be revolutionary if they are consistently used by great powers against one another.

In 2009, monitors discovered that systems and computers associated with the United States Air Force`s Joint Strike Fighter project, also known as the F-35 Lightning II, belonging to Lockheed Martin were compromised. It has never been concretely proven that China was behind the operation; however, the striking similarities between the F-35 and the Chinese J-20 have increased the speculation that China was behind the program

(Council on Foreign Relations, 2020). The goal of this operation was not to destroy or set back the program, the goal was seemingly just for espionage to gain access to the data in order for China to advance its own military aviation program. This use of espionage reiterates the point of the previous paragraph, that this frequent use of espionage takes away from the revolutionary potential of offensive cyber operations because this is simply a new form of information theft in this case, not a new form of warfare.

China has also utilized offensive cyber operations to target people groups that it believes are illegitimate or that they clash with culturally. China conducts these operations domestically, but these operations are outside the scope of this study. These operations are also conducted on an international scale, against these targeted people groups in the sovereign territory of another state, under their protection. In 2018, experts discovered that a threat group in China had been targeting the Tibetan population in India for the purposes of espionage (Council on Foreign Relations, 2020). The Tibetan population is a minority group that China clashes with culturally, but it has very little power. This is an example of China devoting resources to carrying out offensive cyber operations against a weak group of people in another state in order to gain information to use to its advantage. This operation is another incident where a strong actor is acting against a very weak actor/group of people, indicating that offensive cyber operations might not be revolutionary.

The South China Sea is a major area of contention in the region for all of the regional actors, especially China. China has gone to great lengths to assert its supremacy in the region, and conducting offensive cyber operations is no exception. China has at least one, likely several, threat actor groups that work against rivals and targets in the

South China Sea. One of these threat actor groups, APT 30, was discovered in 2015, and targeted over ten state actors in the region. This group is known for utilizing spear-phishing techniques, indicating that these operations were extremely intentional and targeted, not simply wide-net operations that happened to capture these groups as well. These operations could indicate that offensive cyber operations are revolutionary, at least in the sense of a regional conflict. China is able to act against its regional rivals and gain an advantage without carrying out conventional operations.

Based on the available data in the data set, many of China`s offensive cyber operations are conducted against the United States. This could both support and disprove that offensive cyber operations are revolutionary. They are revolutionary in the sense that they allow China to conduct offensive operations against the United States that help them gain an advantage without prompting a conventional conflict. In many of the cases China has also been able to create doubt around their involvement in the operation due to the attribution problem, giving them somewhat of a diplomatic advantage. However, this could also prove that these operations are not revolutionary, or at least not completely. The United States and China are both major powers, allowing these operations to be used as a tool in great power competitions, not weak against strong powers. Many of China`s operations, against the United States and any of its other targets, are also for the purposes of espionage.

Overall Revolutionary Index Data Set Conclusions

The available data that was analyzed in this chapter overall indicates that offensive cyber operations are not revolutionary, at least not in most senses of the term. The *necessary* condition established for them to be considered revolutionary required that most cases should be weaker states carrying out operations against stronger states. While there are a greater number of states that on average carried out operations against states stronger than themselves, the overall number of weaker versus stronger state incidents is lower than the number of stronger versus weaker cases. However, it is not just a matter of stronger versus weaker, there are more nuances that need to be discussed.

Although statistics on the number of states that on average carried out operations against states stronger than themselves and the overall number of operations carried out by weak states against strong nations seem to be at odds with one another, there could be an explanation. The patterns and statistics seem to indicate that the states that utilize offensive cyber operations the most frequently, and potentially the most effectively, are states that are great powers or aspiring great powers. The states generally start out with a certain level of power, there are not cases in the data set of states with little to no power carrying out these operations.

Offensive cyber operations are a way for states that fall into categories of great powers, aspiring great powers, or medium powers to attempt to gain power, or at least an advantage. The main aggressors that on average carried out more offensive cyber operations against stronger states than against weaker states are all aspiring powers. Russia, Iran, and North Korea are all aspiring powers with a level of power already. Though all three of these states have different levels of power, they all aspire to compete on the highest level, against the United States and possibly China, and these operations seem to all them to compete with them in some ways. They utilize these operations to stay relevant as a competitor to other powers and to gain information. However, these operations have not truly changed their power status or taken them past great powers.

In many of the cases of cyber operations in this data set, the operations were used for the purposes of espionage. This does not support the idea that they are revolutionary. Though espionage can give states an advantage, it usually does not change the power balance between the states. The cases seem to indicate that cyber operations are simply a new tool of espionage, not a new tool of warfare. There are claims that offensive cyber operations could be used to shut down power grids and paralyze countries by destroying their means of communication, but these types of operations have not actually occurred to date. There have been denial-of-service incidents that have shut down companies or sectors (such as the Estonian case in 2007), but they have not been to the scale that people have predicted.

In order for offensive cyber operations to be considered truly revolutionary, they need to have actually changed the balance of power or the power dynamic of the world, or at least the states involved. Nuclear weapons are possessed by very few states, but the states that do possess the capability have a certain guarantee of security and level of power. North Korea has nuclear weapons, and they help guarantee its sovereignty to a level that could not be done otherwise. Cyber capabilities do not provide this benefit, and although they can be used in conflict, they do not change the balance of power.

Cyber operations could be seen as revolutionary in the sense that they give aspiring powers a new tool to use against strong powers. However, they could also be seen as not revolutionary since they do not empower weak states and have not caused a shift in the balance of power. The use of these operations as primarily a tool of espionage does not support that these operations are revolutionary either. Though offensive cyber operations might not be truly revolutionary now, it does not mean that they will never be.

The field is still growing quickly, and states are working to develop their capabilities, and the field will continue to evolve.

Chapter Five

Revolutionary Capabilities Data Set Results

After the revolutionary index data was examined, there was a need for further study of what could cause these types of results. Specifically, it is important to examine why some states conduct attacks, some conduct more than others, and other, capable states have conducted no attacks at all. In other words, the following offers an initial statistical examination of which variables affect the propensity of a state to use offensive cyber operations. The Code Book for this data set can be found in Chapter Three. The dependent variable for this analysis was whether or not a state carried out an offensive cyber operation recorded in the Council on Foreign Relations data base from 2005-2019.

The four independent variables were: level of democracy (Freedom House scores); economic power (GDP per capita of each state in US dollars); military power (military expenditure as a percentage of the GDP); and overall state power (Correlates of War Composite Index of National Capabilities (CINC) score). More information about the CINC score is available in chapter three.

The hypotheses based on these variables are as follows:

H1: The higher the level of state power, the more likely that state is to carry out an offensive cyber operation.

H2: The higher the level of military power a state has, the more likely that state is to carry out an offensive cyber operation.

H3: The higher the level of economic power a state has, the more likely that state is to carry out an offensive cyber operation.

H4: The lower the level of democracy of a state, the more likely that state is to carry out an offensive cyber operation.

After loading the data set into R, the variables were vetted. The data is appropriate for statistical analysis and shows signs of convergence. There are some outliers with some of the variables; however, this is expected when dealing with such a wide range of states. The Freedom House variable showed good signs of convergence with no outliers. It shows no signs of overdispersion with a range of 0 to 2 and a standard deviation of .86. The mean is 1.1, the median is 1, and the mode is 2. The GDP per capita variable showed good signs of convergence with only one outlier. The variable shows no signs of overdispersion with a range of $1,098 to $97,341 and a standard deviation of $21,576.26. It has a mean of $25,552, a median of $18,233, and a mode of $49,854.

The CINC score variable showed decent signs of convergence, with eight outliers. These outliers are acceptable because there can be a wide range of state strength within the data set. It shows no signs of overdispersion with a range of 0.000038 to 0.218117 and a standard deviation of .03. The variable has a mean of .01 and a median and mode of 0. The percentage of GDP spent on the military variable showed decent signs of convergence with seven outliers. These outliers are acceptable because some states do spend a much larger percentage of their GDP on their military. The variable shows no signs of overdispersion with a range of 0.2% to 24% with a standard deviation of 3.38. It has a mean of 2.65%, a median of 1.8%, and a mode of .7%.

Each of the 107 cases examined are a state that met the threshold for theoretically being able to carry out an offensive cyber operation. This threshold is based on the state`s military technology listed in the Central Intelligence Agency`s World Factbook, and if the technology listed there requires advanced cyber capabilities to operate, then the state is considered capable of conducting an offensive cyber operation. All 107 of the cases represent states that are capable of conducting offensive cyber operations. Whether or not a state carries out an offensive cyber operation is the dependent variable, scored either 0 for no cyber operation, or 1 for having carried out an offensive cyber operation. For example, one of the cases/data points is China. It has a score of 1 for the dependent variable because it has carried out offensive cyber operations. It has a score of 0 for the Freedom House score because it was rated as not free, and a CINC score of 0.218117. China has a GDP per capita of $16,117 and spends 1.9% of its GDP on the military. All of these points together make up a case.

These relationships between each of the four independent variables and the dependent variable were tested using a logit regression. A logit regression was utilized because the dependent variable is tracked with zeroes and ones, so a linear regression could not be used. There is very limited publicly available information on offensive cyber operations that have been conducted, even those conducted by state actors. If more information on these incidents, such as the length of time of the operation, the level of damage of the operations, and the response by the target state, was available, then a linear regression could be conducted. Conducting a logit analysis is acceptable because there are over 100 cases in the data set.

There are several key limitations associated with the use of a logit model. Due to the binary way in which the dependent variable is measured, with 0s and 1s to represent whether or not a state ever carried out an offensive cyber operation, the scope and frequency of the operations are lost. This data set does not discriminate between one state that carried out one operation that had no effect on another state, and one state that carried out hundreds of operations against other states, some of which were debilitating for the target state. For example, Indonesia was given a score of 1, even though it only carried out one operation against Australia for surveillance, which did not have any major effects on Australia (Council on Foreign Relations, 2020). China was also given a score of 1, but it conducted 118 offensive cyber operations and some of them were debilitating or very damaging for the target, such as when they conducted operations against the United States Office of Personnel Management and gained access to the extensive records of millions of government employees, endangering national security (Council on Foreign Relations, 2020). Both of these states are given the same score utilizing the logit function, which does not at all account for the differences between the two.

When analyzing the logit results, it cannot account for which of the variables have the biggest impact due to logit limitations. In a linear regression the coefficient signifies the strength of the relationship, but it does not in a logit. All that can be solidly determined from the results of the logit analysis is based on the z-value, showing the precision and demonstrating which variables have a real relationship (whether positive or negative). Due to this issue, the coefficient does not indicate how the dependent variables increase or decrease with each change in the independent variable, which makes the results easier to analyze.

The data was analyzed utilizing the R computer program to conduct a logit regression. The threshold for the z-value and confidence level to be considered dependent on each other is 1.96. Only one of the variables crossed this threshold. The following table lists the results of the regression, then the results will be discussed.

Logit Results for Analysis of Determinants of Offensive Cyber Operations				
	Estimate	Standard Error	z value	Pr(>|z|)
(Intercept)	-3.859	0.8619	-4.478	0.00000755
Freedom House	0.4256	0.4264	0.998	0.31825
GDP per Capita	0.00001783	0.0000143	1.241	0.21448
CINC Score	128.1	40.7	3.141	0.00168
Military Spending	0.1482	0.0791	1.873	0.06106

The Freedom House independent variable has neither a precise nor strong relationship with the dependent variable. It has a z-value of 0.988 and a coefficient of 0.426. This indicates that there is not a discernable relationship between the level of democracy and whether or not a state carries out offensive cyber operations. This is both expected and unexpected. A wide variety of states carry out offensive cyber operations, so it is not surprising that there is not a discernable pattern. Democratic states might use these tactics because their populations will not support conventional offensive operations against another state to spark an armed conflict, they do not respond as positively to these actions. Less democratic states might use these tactics because they are able to exploit the systems and societies of states with more freedoms to their advantage. The lack of a relationship between the level of democracy of a state and whether or not it chooses to carry out offensive cyber operations will not help people predict what states are more likely to use these tactics. These results do not support Hypothesis 4.

The economic power independent variable that is measured by the GDP per capita of each state has neither a precise nor a strong relationship with the dependent variable. It has a z-value of 1.241 and a coefficient of 0.00001783. This disproves Hypothesis 3, which stated that the more economic power a state has, the more likely it would be to carry out an offensive cyber operation. While the z-value does not meet the standard, this economic power variable has a more precise and strong relationship with the dependent variable than the level of democracy. An economically powerful state might use offensive cyber operations to advance their economic standing further. An economically weak state might use offensive cyber operations to advance its economic standing by stealing intellectual property or proprietary information from another state. Economically weak states might have been more likely to carry out offensive cyber operations because they are cheaper than other methods to gain power and do not cost a large amount of money. Since both economically strong and economically weak states have the motivation, and likely the means, to carry out these operations, the lack of a strong relationship could be expected.

The military power independent variable that is measured by the percentage of the GDP spent on the military by each state is not strong and does not meet the 1.96 threshold for precision, but it is very close, with a z-value of 1.873. It has a coefficient of 0.1482. Although the z-value of 1.873 does not reach the threshold of 1.96, it crosses the 90% threshold so it can be considered to have a significant relationship with the dependent variable. It could be a determining or predictive factor of which states will carry out offensive cyber operations. Since this variable reaches the 90% threshold, it qualifies as significant (though less so than if it crossed the 1.96 threshold), it supports the findings of the previous chapter that the stronger states (who would be strong militarily) are more likely to carry out more offensive cyber operations. Hypothesis 2 was partly supported suggesting an avenue for future research.

The overall level of power, measured by the Correlates of War Composite Index of National Capabilities (CINC) score, was the only independent variable that crossed the

1.96 threshold. This independent variable has a z-value of 3.141 and a coefficient of 128.1. This indicates that there is a high level of precision between the overall level of power and whether or not a state carries out offensive cyber operations. The relationship is positive, indicating that the stronger a state is, the more likely that state is to carry out an offensive cyber operation. This would support the results of the previous chapter for a number of reasons. This independent variable utilized the same metric as the revolutionary index capabilities data set. The results of the regression of this independent variable with the dependent variable support the idea of the revolutionary capabilities data set because both indicate that the stronger a state is, the more likely it is to carry out offensive cyber operations. The z-value of 3.141 is significantly higher than 1.96, indicating that this relationship is statistically significant.

Based on the two independent variables that have a significant relationship with the dependent variable, five different models were estimated to determine the likelihood that a nation would carry out an offensive cyber operation. Since the CINC score and percentage of GDP spent on the military were the two variables that had relationships with whether or not a nation carried out an offensive cyber operation, they were each varied by half of a standard deviation and one standard deviation in order to determine predictive values. The following table presents the probabilities determined for each variation of the independent variables:

Probability Table	
Average	10.1%
+1/2 standard deviation of CINC score	43.4%
+1 standard deviation of CINC score	84%
+1/2 standard deviation of military	12.6%
+1 standard deviation of military	15.6%

These results demonstrate that the CINC score variable has a much greater effect on the dependent variable than the military expenditure variable. This supports that for each increase in overall nation power, the probability that the nation will carry out an offensive cyber operation increases significantly. An increase in military expenditure could also relate to an increase in the likelihood that a nation will conduct an offensive cyber operation, but the relationship does not appear to be as closely linked as overall nation power.

The results of this data set indicate that the level of democracy and economic power do not have an effect on whether or not a state carries out offensive cyber operations. While military power does not quite meet the threshold, it is close enough to the 1.96 threshold to be worthy of consideration in future studies. The only variable that unambiguously achieves statistical significance is overall state power.

Chapter Six

Conclusion

The goal of this paper was to determine if offensive cyber operations are revolutionary tools of warfare. There is a significant amount of future research to be conducted in this area, but this study provides a starting point. It began by analyzing the existing data base of offensive cyber operations compiled by the Council on Foreign Relations in the Revolutionary Index Data Set. Based on this data set, offensive cyber operations are not revolutionary tools of warfare because (based on publicly available data) the states that carry out most of the offensive cyber operations are already strong states, or at least states that have some level of world standing already.

While this data could also cause offensive cyber operations to be considered revolutionary in the sense that states were still conducting operations against states stronger than themselves, most of these states already had some level of power. This indicates that it is a tool used by great powers, or aspiring great powers, to gain or maintain power, which does not make it revolutionary. The main states that conducted offensive cyber operations were China, the United States, Russia, Iran, and North Korea. All of these states are either great powers or aspiring great powers. If many states that have little or no power conducted a large number of operations or even just a few operations against major powers, then these operations might be considered revolutionary. However, this is not the case, so these operations are not revolutionary.

After this data set was examined, it led to the need for further examination of the factors that might have caused the results of the Revolutionary Index Data Set, which lead to the Revolutionary Capabilities Data Set. This examined the effects of four different variables on whether or not a state chooses to carry out offensive cyber operations: level of democracy, economic power, military power, and overall state power. The results of the Revolutionary Capabilities Data Set indicate that out of these four variables, only overall state power is correlated with whether or not a nation chooses to carry out offensive cyber operations. Military power comes close to the threshold to be considered a significant and relevant factor, but only overall state power crosses the threshold. The relationship between the overall state power and whether or not a state carries out offensive cyber operations is positive, indicating that the more power a state has, the more likely it is to carry out on offensive cyber operation.

Overall state power meeting the requirements to be considered a relevant and significant factor fits in with the results of the Revolutionary Index Data Set as well. The overall state power variable was measured with the same data/measure as the Revolutionary Index Data Set: the CINC score from the Correlates of War database. This also demonstrates that the results of the Revolutionary Capabilities Data Set match the results of the Revolutionary Index Data Set. The stronger a state is, the more likely that state is to carry out an offensive cyber operation.

If stronger states are more likely to carry out offensive cyber operations, this means that offensive cyber operations are not revolutionary tools of warfare. If weaker states were more likely to carry out offensive cyber operations or were at least as likely as stronger states, then this would meet the necessary condition for cyber attacks to be considered revolutionary. However, since this is not the case, these operations cannot be deemed reovlutionary. Further study of this topic could yield different results but based on the parameters and scope of this study, offensive cyber operations cannot be considered revolutionary.

Through these two data sets, this study demonstrated that offensive cyber operations are not equalizing tools utilized by smaller and weaker states, at least not to a level worth noting. They are utilized by some relatively weaker states, but rarely and not by any truly weak states. For example, the data sets did not demonstrate instances of African or South American states utilizing these operations against one another, or against major world powers such as the United States and China. These types of operations would indicate a revolutionary capability, but there was no evidence of them in the available data.

This will serve as a starting point to help guide future research on which states or types of states conduct offensive cyber operations. The field of cyber operations will continue to evolve over time, likely quickly. As more data becomes available, this study and studies like this will be able to be carried out more accurately and with better data. Even though this study has concluded that offensive cyber operations are not revolutionary, this does not mean that these operations will not be revolutionary in the future. As more states gain more capabilities, and more extensive capabilities, they might be more likely to conduct offensive cyber operations to gain more power. It is also possible that cyber operations will become normal and expected tools in conflicts. There are many possibilities for the future of offensive cyber operations and the study of them, this study is only portion of the beginning of the area.

Appendix

Numbers of Offensive Cyber Operations by State

Australia	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	0
2019	1
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.032781

Canada	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	0
2019	1
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.030924

China	
2005	1
2006	3
2007	6
2008	5
2009	3
2010	4
2011	9
2012	5
2013	9
2014	14
2015	11
2016	5
2017	6
2018	17
2019	20
Total Number of Offensive Operations	118
Average Revolutionary Index Score	-0.145177

France	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	1
2015	0
2016	0
2017	0
2018	0
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.023427

India	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	1
2014	0
2015	0
2016	0
2017	0
2018	0
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	-0.040029

Indonesia	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	1
2017	0
2018	0
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	-0.007149

Iran	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	3
2011	0
2012	4
2013	1
2014	5
2015	4
2016	2
2017	5
2018	4
2019	8
Total Number of Offensive Operations	36
Average Revolutionary Index Score	0.050532

Israel	
2005	0
2006	0
2007	1
2008	0
2009	0
2010	1
2011	1
2012	2
2013	0
2014	0
2015	1
2016	0
2017	1
2018	0
2019	0
Total Number of Offensive Operations	7
Average Revolutionary Index Score	0.009568

Lebanon	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	1
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.044187

Netherlands	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	1
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.035942

New Zealand	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	0
2019	1
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.039217

North Korea	
2005	0
2006	0
2007	0
2008	0
2009	1
2010	0
2011	2
2012	0
2013	2
2014	1
2015	2
2016	3
2017	4
2018	6
2019	6
Total Number of Offensive Operations	27
Average Revolutionary Index Score	0.045054

Pakistan	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	4
2019	0
Total Number of Offensive Operations	4
Average Revolutionary Index Score	0.062580

Russia	
2005	0
2006	0
2007	2
2008	2
2009	0
2010	0
2011	0
2012	0
2013	4
2014	6
2015	9
2016	9
2017	15
2018	20
2019	8
Total Number of Offensive Operations	75
Average Revolutionary Index Score	0.006260

South Korea	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	1
2015	0
2016	0
2017	0
2018	0
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.053549

Spain	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	1
2015	0
2016	0
2017	0
2018	0
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.011283

Syria	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	1
2015	0
2016	0
2017	0
2018	0
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.134512

Taiwan	
2005	0
2006	0
2007	1
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	0
2019	0
Total Number of Offensive Operations	1
Average Revolutionary Index Score	0.178149

United Arab Emirates	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	1
2018	0
2019	1
Total Number of Offensive Operations	2
Average Revolutionary Index Score	0.000951

United Kingdom	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	1
2015	0
2016	0
2017	0
2018	0
2019	1
Total Number of Offensive Operations	2
Average Revolutionary Index Score	0.012904

United States	
2005	0
2006	0
2007	1
2008	0
2009	0
2010	1
2011	0
2012	2
2013	0
2014	1
2015	1
2016	1
2017	2
2018	0
2019	4
Total Number of Offensive Operations	13
Average Revolutionary Index Score	-0.106330

Vietnam	
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	3
2016	0
2017	0
2018	0
2019	1
Total Number of Offensive Operations	4
Average Revolutionary Index Score	0.071101

State Cases in the Revolutionary Capabilities Data Set

Afghanistan	Kenya
Angola	Korea, North
Argentina	Korea, South
Armenia	Kuwait
Australia	Kyrgyzstan
Austria	Laos
Azerbaijan	Latvia
Bahrain	Lebanon
Bangladesh	Libya
Belarus	Lithuania
Belgium	Malaysia
Bolivia	Mexico
Bosnia and Herzegovina	Mongolia
Botswana	Montenegro
Brazil	Morocco
Bulgaria	Myanmar
Cambodia	Netherlands
Cameroon	New Zealand
Canada	Nigeria
Chad	Norway
Chile	Oman
China	Pakistan
Colombia	Peru
Croatia	Poland
Cuba	Portugal
Cyprus	Qatar
Czech Republic	Romania
Democratic Republic of the Congo	Russia
Denmark	Saudi Arabia
Ecuador	Serbia
Egypt	Singapore
Eritrea	Slovak Republic
Estonia	South Africa
Ethiopia	Spain
Finland	Sweden
France	Switzerland
Gabon	Syria
Georgia	Taiwan
Germany	Tanzania
Ghana	Thailand
Greece	Tunisia
Honduras	Turkey
Hungary	Uganda
Iceland	Ukraine

India	United Arab Emirates
Indonesia	United Kingdom
Iran	United States
Iraq	Uzbekistan
Ireland	Venezuela
Israel	Vietnam
Italy	Yemen
Japan	Zambia
Jordan	Zimbabwe
Kazakhstan	

Bibliography

Barrett, B. (2020, December 19). *Security News This Week: Russia`s SolarWinds Hack is a Historic Mess*. WIRED. https://www.wired.com/story/russia-solarwinds-hack-roundup/

Borghard, E. & Lonergan, S. (2017). The Logic of Coercion in Cyberspace. *Security Studies, 26*(3), 452-481. DOI: 10.1080/09636412.2017.1306396

Buchanan, B. (2016). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Burton, J. (2015). NATO`s cyber defense: strategic challenges and institutional adaptation. *Defense Studies, 15*(4), 297-318. DOI:10.1080/14702436.2015.1108108

Choucri, N. & Clark, D. (2018). *International Relations in the Cyber Age*. The MIT Press.

Clarke, R. and Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins Publishers.

Colarik, A. and Janczewski, L. (2011, August 15-17). *Developing a Grand Strategy for Cyber War* [Conference Presentation]. International Conference on Information Assurance and Security, Brno, Czech Republic.

Council on Foreign Relations. (2020, August 20). *Cyber Operations Tracker*. Council on Foreign Relations. https://www.cfr.org/interactive/cyber-operations

Davis, N. (1996). An Information-Based Revolution in Military Affairs. *Strategic Review, 24*(1), 43-53.

Echevarria II, A. (2017). *Military Strategy: A Very Short Introduction*. Oxford University Press.

Friedman, A. and Singer, P.W. (2014). *Cyber Security and Cyber War: What Everyone Needs to Know*. Oxford University Press.

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory Than in Practice? *Strategic*

Studies Quarterly, 4(3), 102-135. Retrieved from: https://www.jstor.org/stable/10.2307/26269789

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin`s Most Dangerous Hackers*. Penguin Random House LLC.

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation, and Technology, 9*(2), 159-189. DOI:10.1080/17579961.2017.1377914

Harris, S. (2014). *@War: The Rise of the Military-Internet Complex*. Houghton Mifflin Harcourt Publishing.

Hautala, L. (2021, January 5). *SolarWinds hack officially blamed on Russia: What you need to know*. CNet. https://www.cnet.com/news/solarwinds-hack-officially-blamed-on-russia-what-you-need-to-know/#:~:text=The%20massive%20breach%2C%20which%20reportedly,IT%20management%20software%20from%20SolarWinds.

Herzog, S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49-60. DOI:10.5038/1944-0472.4.2.3

Jervis, R. Cooperation Under the Security Dilemma. *World Politics, 30*(2), 167-214.

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*. Simon & Schuster Paperbacks.

Kshetri, N. (2016). *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*. Springer International Publishing.

McGavran, W. (2009). Intended consequences: Regulating cyber attacks. *Tulane Journal of Technology and Intellectual Property, 12*(1), 259-276.

Matisek, J. (2017). Shades of Gray Deterrence: Issues of Fighting in the Gray Zone. *Journal of Strategic Security, 10*(3), 1-26. DOI: 10.5038/1944-0472.10.3.1589.

Merriam-Webster. (n.d.). Revolutionary. In Merriam-Webster.com dictionary. Retrieved January 30, 2021, from https://www.merriam-webster.com/dictionary/revolutionary

Osawa, J. The Escalation of State Sponsored Cyberattack and National Cyber Security

Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review, 24*(2), 113-131. DOI: 10.1080/13439006.2017.1406703.

Perlroth, N. (2020, December 24). *Russians Are Believed to Have Used Microsoft Resellers in Cyber Attacks*. New York Times. https://www.nytimes.com/2020/12/24/us/russia-microsoft-resellers-cyberattacks.html

Poznansky, M. & Perkoski, E. (2018). Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution. *Journal of Global Security Studies, 3*(4), 402-416. DOI: 10.1093/jogss/ogy022

Rustici, R. (2011). Cyberweapons: Leveling the International Playing Field. *Parameters*, 32-42.

Ruttan, V. (2006). *Is War Necessary for Economic Growth?* Oxford University Press.

Sanger, D. (2021, January 2). *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*. New York Times. https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html

Sanger, D. & Perlroth, N. (2021, January 5). *As Understanding of Russian Hacking Grows, So Does Alarm.* New York Times. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

Schmidt, M. & Sanger, D. & Perlroth, N. (2014, July 2). *Chinese Hackers Pursue Key Data on U.S. Workers*. New York Times. https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0

Sciutto, J. (2019). *The Shadow War*. HarperCollins Publishers.

Sebenius, A. (2019, October 4). Microsoft Says Iran Tried Hack of U.S. Presidential Campaign. Bloomberg. https://www.bloomberg.com/news/articles/2019-10-04/microsoft-says-iran-tried-to-hack-a-u-s-presidential-campaign

Sethi, V. (2020). *Cyber Weapons of Mass Psychological Destruction*. Greylander Press.

Sharma, A. (2010). Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis, 34*(1), 62-73. DOI: 10.1080/09700160903354450

Singer, J. & David, S. & and Stuckey, J. (1972). "Capability Distribution, Uncertainty, and Major Power War, 1820-1965." in Bruce Russett (ed) Peace, War, and

Numbers, Beverly Hills: Sage, 19-48.

Valeriano, B. & Jensen, B. & Maness, R. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.

Valeriano, B. & Maness, R. & Jensen, B. (2020, September 06). *The Dyadic Cyber Incident and Dispute Data, Versions 1, 1.1, and 1.5*. Ryan C. Maness, PhD. https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset

Vaughan-Nichols, S. (2021, January 4). *SolarWinds: The more we learn, the worse it looks*. ZDNet. https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/

Whyte, C. (2020). Beyond tit-for-tat in cyberspace: Political warfare and lateral sources of escalation online. *European Journal of International Security, 5*, 195-214. DOI: 10.1017/eis.2020.2